ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 202x

Part 1: Introduction

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 1 — *Introduction*
ISBN 978-92-9249-790-3

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

1. FOREWORD

ICAO's work on machine readable travel documents began in 1968 with the establishment, by the Air Transport Committee of the Council, of a Panel on Passport Cards. This Panel was charged with developing recommendations for a standardized passport book or card that would be machine readable, in the interest of accelerating the clearance of passengers through passport controls. The Panel produced a number of recommendations, including the adoption of optical character recognition (OCR) as the machine reading technology of choice due to its maturity, cost-effectiveness and reliability. In 1980, the specifications and guidance material developed by the Panel were published as the first edition of Doc 9303, titled *A Passport with Machine Readable Capability*, which became the basis for the initial issuance of machine readable passports by Australia, Canada and the United States.

In 1984, ICAO established what is now known as the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), comprised of government officials who specialize in the issuance and border inspection of passports and other travel documents, in order to update and enhance the specifications which had been prepared by the Panel. Subsequently, this group's terms of reference were expanded to include, first, the development of specifications for a machine readable visa and, later, specifications for machine readable cards that may be used as official travel documents.

In 1998, the New Technologies Working Group of the TAG/MRTD began work to establish the most effective biometric identification system and associated means of data storage for use in MRTD applications, particularly in relation to document issuance and immigration considerations. The bulk of the work had been completed by the time the events of 11 September 2001 caused States to attach greater importance to the security of a travel document and the identification of its holder. The work was quickly finalized and endorsed by the TAG/MRTD and the Air Transport Committee.

The resulting Technical Reports on the employment of biometrics and contactless chip technology, Logical Data Structure (LDS), and Public Key Infrastructure (PKI) were incorporated into Volume 2 of the Sixth Edition of Doc 9303, Part 1 (*Machine Readable Passports*) in 2006, and Volume 2 of the Third Edition of Doc 9303, Part 3 (*Machine Readable Official Travel Documents*) in 2008.

2. SCOPE

Doc 9303 consists of various separate documents in which general (applicable to all MRTDs) as well as MRTD form factor specific specifications are grouped. See Section 5.1 "Doc 9303 Composition" for an overview.

These specifications are not intended to be a standard for national identity documents. However, a State whose identity documents are recognized by other States as valid travel documents shall design its identity documents such that they conform to the specifications of Doc 9303-3 and Doc 9303-4, Doc 9303-5 or Doc 9303-6.

Although the specifications in Doc 9303-4 are intended for particular application to the passport, these specifications apply equally to other TD3 size identity documents, for example, the laissez-passer, the seafarer's identity document and refugee travel documents.

The document at hand is Part 1. Part 1 introduces the Doc 9303 specifications. It describes the build-up of the thirteen parts of Doc 9303, provides general information on ICAO, and guidance on the terminology and abbreviations used throughout the specifications.

3. GENERAL CONSIDERATIONS

3.1 ICAO's Leadership Role

ICAO's initiative to develop standard specifications for passports and other travel documents followed the tradition established by the League of Nations Passport Conferences of the 1920s and the work of the League's successor, the United Nations Organization. ICAO's mandate to continue in its leadership role stems from the Convention on International Civil Aviation (the "Chicago Convention") which covers the full range of requirements for efficient and orderly civil aviation operations, including provisions for clearance of persons through border controls, i.e.:

a) the requirement for persons travelling by air and aircraft crews to comply with immigration, customs and passport regulations (Article 13);

b) the requirement for States to facilitate border clearance formalities and prevent unnecessary delays (Article 22);

c) the requirement that States collaborate in these matters (Article 23); and

d) the requirement for States to develop and adopt internationally standard procedures for immigration and customs clearance (Article 37 j)).

Under this mandate, ICAO develops and maintains international Standards in Annex 9 — *Facilitation* to the Chicago Convention for implementation by Member States. In the development of such Standards, it is a fundamental precept that if public authorities are to facilitate inspection formalities for the vast majority of air travellers, those authorities must have a satisfactory level of confidence in the reliability of travel documents and in the effectiveness of inspection procedures. The production of standardized specifications for travel documents and the data contained therein is aimed at building that confidence.

In 2004, the Assembly of ICAO affirmed that cooperative work on specifications to strengthen the security and integrity of travel documents should be pursued by the Organization as a matter of high priority. In addition to the International Organization for Standardization (ISO), consultants to the TAG/MRTD include the International Air Transport Association (IATA), the Airports Council International (ACI), and the International Criminal Police Organization (INTERPOL).

In 2005, the then 188 Member States of ICAO approved a new Standard that all States must begin issuing machine readable passports in accordance with Doc 9303 no later than the year 2010. No later than the year 2015 all non-machine readable travel documents must have expired. This Standard is published in the 13th Edition (2011) of Annex 9 — *Facilitation*.

3.2 Relative Costs and Benefits of Machine Readable Travel Documents

Experience with the issuance of machine readable passports, in conformity with the specifications set forth in Doc 9303, indicates that the cost of producing MRTDs may be no greater than that of producing conventional documents, though the cost will be higher when biometric identification and electronic travel documents are implemented. As traffic volumes grow and more States focus on how they can rationalize their clearance processes with the employment of computerized databases and electronic data interchange, the MRTD plays a pivotal part in modern, enhanced compliance systems. Equipment to read the documents and access the databases may entail a substantial investment, but this can be expected to be returned by the improvements in security, clearance speed and accuracy of verification which such systems provide. Use of MRTDs in automated clearance systems may also make it possible for States to eliminate both the requirement for paper documents, such as passenger manifests and embarkation/disembarkation cards, and the administrative costs associated with the related manual procedures.

3.3 Operations

The basic machine readable travel document, with its OCR readability, is designed for both visual and mechanical reading.

ICAO Member States have recognized that standardization is a necessity and that the benefits of adopting the Doc 9303 standard formats for passports and other travel documents extend beyond the obvious advantages for States that have the machine readers and databases for use in automated clearance systems. In fact, the physical characteristics and data security features of the documents themselves offer strong defence against alteration, forgery or counterfeit. Moreover, adoption of the standardized format for the visual zone of an MRTD facilitates inspection by airline and government officials, with the result that clearance of low-risk traffic is expedited, problem cases are more readily identified, and enforcement is improved. The optional introduction of biometric identification with data stored on a contactless integrated circuit will provide greater security and resistance to fraud and thus make it easier for the legitimate document holder to obtain visas for travel and to be processed through border inspection systems.

Note.— It is recognized that situations will arise where an eMRTD will not interface correctly with a reader at a border. There are several reasons why this might occur, of which a failure of the eMRTD is only one. ICAO emphasizes that an eMRTD which fails to read is nevertheless a valid document. However, a failure to read could be the result of fraudulent attack, and the receiving State should establish its own procedures for dealing with this possibility, which should involve more stringent inspection of the document and its holder but also allow that the failure involves no fraudulent intent.

3.5 Endorsement by ISO

The technical specifications sections of Doc 9303 have received the endorsement of the International Organization for Standardization as ISO Standard 7501. Such endorsement is made possible by means of a liaison mechanism through which manufacturers of travel documents, readers and other technologies provide technical and engineering advice to the TAG/TRIP under the auspices of ISO. Through this working relationship, the ICAO specifications have achieved, and are expected to continue to receive, the status of worldwide standards by means of a simplified procedure within ISO.

The liaison mechanism with ISO has been successfully applied not only to the endorsement of new specifications for travel documents as ISO standards but also to the approval of amendments to the specifications. Subsequent revisions to Doc 9303 will therefore be processed for ISO endorsement in the same manner as previously.

4. DEFINITIONS AND REFERENCES

4.1 Acronyms

Acronym	Full form
3DES	Triple DES
AA	Active Authentication
ABC	Automated Border Control
AFS	Anti-Fraud Specialist
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application Protocol Data Unit
AO	Authorizing Officer
BAC	Basic Access Control
BER	Basic Encoding Rules
BLOB	Binary Large Object
BSC	Bar Code Signer Certificate
CA	Certification Authority – also – Chip Authentication
CAM	Chip Authentication Mapping
CAN	Card Access Number
CAR	Certification Authority Reference
CBC	Cypher Block Chaining
CBEFF	Common Biometric Exchange Format Framework
CCD	Charge-Coupled Device
C_{DS}	Document Signer Certificate
CIC	Contactless Integrated Circuit
CID	Card IDentifier
CMAC	Cipher-based Message Authentication Code
CMOS	Complementary Metal–Oxide–Semiconductor
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CSD	Camera to Subject Distance; distance between the eyes plane of a person and the optical center of the camera lens
CVCA	Country Verifying Certification Authority
DER	Distinguished Encoding Rule

Acronym	Full form
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie Hellmann
DN	Distinguished Name
DO	Data Object
DOVID	Diffractive Optically Variable Image Device (Feature with diffractive optically variable effects, e.g. holographic effects)
DS	Document Signer
DSA	Digital Signature Algorithm
DTA	Digital Travel Authorization
DTBS	Data To Be Signed
DV	Document Verifier
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie Hellmann
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA	Elliptic Curve Key Agreement
EEPROM	Electrically Erasable Programmable Read Only Memory
EF	Elementary File
EM	Eye to Mouth distance
eMRP	Electronic Machine Readable Passport
eMRTD	Electronic Machine Readable Travel Document
eMROTD	Electronic Machine Readable Official Travel Document
eRP	Electronic Residence Permit
ERZ	Effective Reading Zone
ETS	Electronic Travel System
EVZ	Eye visibility zone; zone covering a rectangle having a distance V of at least 5% of the IED to any part of the visible eye ball
FAR	False Acceptance Rate
FIPS	Federal Information Processing Standard
FRR	False Rejection Rate
GM	Generic Mapping
HD	Horizontal deviation angle; maximal allowed deviation from the horizontal of the imaginary line between the nose of a person and the lens of the camera

Acronym	Full form
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IED	Inter Eye Distance
IFD	InterFace Device
IM	Integrated Mapping
IR	InfraRed light
IS	Inspection System
IV	Initial Vector
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRP	Machine Readable Passport
MRTD	Machine Readable Travel Document
MROTD	Machine Readable Official Travel Document in the form of a card
MRV-A	Full size (Format A) Machine Readable Visa
MRV-B	Small size (Format B) Machine Readable Visa
MRZ	Machine Readable Zone
MTF	Modulation Transfer Function
MTF20	Highest spatial frequency where the MTF is 20% or above
NAD	Node ADdress
NIST	National Institute of Standards and Technology
NTWG	New Technologies Working Group
OCR	Optical Character Recognition
OCR-B	Optical Character Recognition font defined in ISO 1073-2
OID	Object IDentifier
OVD	Optically Variable Device
OVI	Optically variable ink
OVF	Optically Variable Feature
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
RFID	Radio Frequency IDentification
PICC	Proximity Integrated Circuit Card

Acronym	Full form
PIX	Proprietary Identifier eXtension (PIX).
PKD	Public Key Directory
PKI	Public Key Infrastructure
RGB	Red-Green-Blue
RID	Registered IDentifier (RID)
ROI	Region Of Interest
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
SFR	Spatial Frequency Response
SHA	Secure Hash Algorithm
SM	Secure Messaging
SNR	Signal to Noise Ratio
SO_D	Document Security Object
SPOC	Single Point Of Contact
sRGB	standard RGB colour space created for use on monitors, printers and the Internet using the ITU-R BT.709 primaries
SSC	Send Sequence Counter
TA	Terminal Authentication
TAG/MRTD	Technical Advisory Group on Machine Readable Travel Documents
TAG/TRIP	Technical Advisory Group on the TRaveller Identification Programme
TD1	Size 1 Machine Readable Official Travel Document
TD2	Size 2 Machine Readable Official Travel Document
TD3	Size 3 Machine Readable Travel Document
TLV	Tag Length Value
TR	Technical Report
UID	Unique IDentifier
UV	UltraViolet light
VDS	Visible Digital Seal
VIS	Visa Information System of the European Union.
VIZ	Visual Inspection Zone
VS	Visa Signer
VVA	Visa Validation Authority
WSQ	Wavelet Scalar Quantization

4.2 Terms and Definitions

Term	Definition
1:1 application case	Biometric process (algorithm) comparing a sample photo with a registered sample of the claimed identity, also known as verification.
1:N application case	Biometric process (algorithm) searching an a priori unknown sample photo among N registered samples in a database, also known as identification.
ABC gate	Automated Border Control Gate for electronic machine readable travel documents.
Adobe RGB	RGB colour space designed to encompass most of the colours achievable on CMYK colour printers, but by using RGB primary colours on a device such as a computer display
Algorithm	A specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.
Anti-scan pattern	An image usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the image cannot be distinguished from the remainder of the background security print but when the original is scanned or photocopied the embedded image becomes visible.
Application Identifier (AID)	Data element that identifies an application. eMRTD applications use a Standard AID that is one of four categories of AID. It consists of a registered application provider identifier (RID) and a proprietary application identifier extension (PIX).
Asymmetric	Different keys needed on each end of a communication link.
Asymmetric algorithm	This type of cryptographic operation uses one key for encryption of plain text and another key for decryption of associated cipher text. These two keys are related to each other and are called a Key Pair.
Asymmetric keys	A separate but integrated user key pair comprised of one public key and one private key. Each key is one-way, meaning that a key used to encrypt information cannot be used to decrypt the same information.
Authentication	A process that validates the claimed identity of a participant in an electronic transaction.
Authentication Database	In this database the authentication algorithms for the implementation of the check routines are stored for each document model.
Authentication Dataset	A specific set of check routines for a document model within the authentication data-base.
Authenticity	The ability to confirm that the Logical Data Structure and its components were created by the issuing State or organization.
Authorization	A security process to decide whether a service can be given or not.
Authorization to travel	Either a non-physical and/or a physical authorization issued by the receiving state authorizing the traveller to travel.
Authorized receiving organization	Organization authorized to process an official travel document (e.g. an aircraft operator) and, as such, potentially allowed in the future to record details in the optional capacity expansion technology.
Bar code	Optical, machine-readable representation, in one or two dimensions, of data relating to the

Term	Definition
	object to which it is attached.
Bar code signer	A bar code Signer digitally signs the data (header and message) encoded in the bar code. The signature is also stored in the bar code.
Bar Code Signer Certificate (BSC)	A BSC is a certificate that contains the bar code Signer's public key. Bar code Signer certificates are used to verify the validity of data that were signed with the bar code Signer's private key.
Bar Code Symbology	A mapping between messages and bar codes is called a symbology. Such mapping is defined in the specification of the bar code and includes the encoding of single digits or characters, the size of a so called quiet zone around the bar code, as well as the computation of checksums for error correction.
Biographical data (biodata)	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the MRTD, or on the chip if present.
Biometric	A measurable, unique, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrollee.
Biometric Data	The information extracted from the biometric and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).
Biometric Identification	A means of identifying or confirming the identity of the holder of an MRTD by the measurement of one or more properties of the holder’s person.
Biometric matching	The process of using an algorithm that compares templates derived from the biometric reference and from the live biometric input, resulting in a determination of match or non-match.
Biometric reference template	A data set which defines a biometric measurement of a person which is used as a basis for comparison against a subsequently submitted biometric sample(s).
Biometric sample	Raw data captured as a discrete, unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).
Biometric system	An automated system capable of: 1. capturing a biometric sample from an end user for an MRP; 2. extracting biometric data from that biometric sample; 3. comparing that specific biometric data value(s) with that contained in one or more reference templates; 4. deciding how well the data match, i.e. executing a rule-based matching process specific to the requirements of the unambiguous identification and person authentication of the enrollee with respect to the transaction involved; and 5. indicating whether or not an identification or verification of identity has been achieved.
Biometric template	Extracted and compressed data taken from a biometric sample.
Biometric verification	A means of identifying or confirming the identity of the holder of an MRTD by the measurement and validation of one or more unique properties of the holder’s person.

Term	Definition
Bit	A binary digit. The smallest possible unit of information in a digital code.
Black-line white-line design	A design made up of fine lines often in the form of a guilloche pattern and sometimes used as a border to a security document. The pattern migrates from a positive to a negative image as it progresses across the page.
Block	A string or group of bits that a block algorithm operates on.
Block algorithm	See: block cipher.
Block cipher	Algorithms that operate on plain text in blocks (strings or groups) of bits.
Bootstrapping	A method of testing the reliability of a data set.
Breeder Document	Documentation used as evidence of identity when applying for a travel document.
Brute-force attack	Trying every possible key and checking whether the resulting plain text is meaningful.
Byte	A sequence of eight bits usually operated on as a unit.
Caption	Printed word or phrase to identify a data field. In exceptional circumstances, when multiple different official languages do not fit in the data field, numbers can be used. These numbers must be accompanied by explanatory text at another location in the MRP.
Capture	The method of taking a biometric sample from the end user.
Card	Medium according to ISO/IEC 7810, ISO/IEC 7811, ISO 7812 used to carry information.
Certificate	Electronic file attesting that a cryptographic key pair belongs to a person or a hardware or software component as identified in the certificate. A certificate is issued by a Certification Authority. By signing the certificate, the Certification Authority approves the link between the identity of a person or component and the cryptographic key pair. The certificate may be revoked if it doesn't attest the validity of this link any more. The certificate has a limited validity period.
Certificate Revocation List (CRL)	A list of certificates that have been revoked. Documents associated to (signed by) a certificate contained in a CRL SHALL thus no longer be trusted.
Certification Authority (CA)	A trustworthy body that issues digital certificates for PKI.
Check algorithm	Software components which enable the specific implementation of check routines (e.g. search for patterns).
Check routine	Testing procedure for a feature’s specific property (e.g. examination for the presence of the photo in IR-light).
Chemical sensitizers	Security reagents to guard against tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.
Chin	Central forward portion of the lower jaw.
CIE Standard Illuminant D65	Commonly used standard illuminant defined by the International Commission on Illumination (CIE) that is part of the D series of illuminants trying to portray standard illumination conditions at open-air in different parts of the world.

Term	Definition
Cipher	Secret writing based on a key, or set of predetermined rules or symbols.
Collation marks	See: Index marks.
Colour shifting ink	Inks changing their visual characteristic depending on the viewing angle and/or the quality of a stimulating (light) source.
Comparison	The process of comparing a biometric sample with a previously stored reference template or templates. See also “One-to-many” and “One-to-one”.
Contactless integrated circuit	A semi-conductor device which stores MRTD data and which communicates with a reader using radio frequency energy according to ISO/IEC 14443.
Common Biometric Exchange Format Framework (CBEFF)	A common file format that facilitates exchange and interoperability of biometric data.
Control Number	A number assigned to a document at the time of its manufacture for record-keeping and security purposes.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country code	A two- or three-letter code as defined in ISO 3166-1, used to designate a document issuing authority or nationality of the document holder.
Crop factor	Ratio of the diagonal of the full frame camera (43.3 mm) to that of a selected camera’s image sensor. The determination of an appropriate focal length lens for a field of view equivalent to a full frame camera can be made by considering the crop factor.
Crown	Top of the head ignoring any hair.
Cryptography	Science of transforming information into an enciphered, unintelligible form using an algorithm and a key.
Data Group	A series of related Data Elements grouped together within the Logical Data Structure.
Data Encryption Standard (DES)	A method of data encryption specified in FIPS 46-3.
Data Feature	The incorporation of encoded information into the document data or image structure, usually into the personalization data, especially the portrait.
Data Page	The page of the passport book, preferably the second or penultimate page, which contains the biographical data of the document holder. See “Biographical data”.
Data To Be Signed (DTBS)	The message that is given as input to a signature generation algorithm of a signature scheme.
Decryption	The act of restoring an encrypted file to its original state through the use of a key.
Deviation List	Signed list issued by an issuing State specifying non-conformities in travel documents and/or keys and certificates.
Deviation List Signer	An entity that digitally signs a Deviation List. The Deviation List signer is authorized by its national CSCA to perform this function through the issuance of a Deviation List Signer

Term	Definition
	certificate.
Diffractive Optically Variable Device	A security feature containing a holographic or equivalent image within its construction, the image changing its appearance with angle of viewing or illumination.
Diffractive Optically Variable Image Device (DOVID) Laminate or Overlay	A laminate or overlay containing a DOVID either covering a whole area or located so as to protect key data on the document.
Digital (cryptographic) signature	The result of a cryptographic operation enabling the validation of information by electronic means. This is NOT the displayed signature of the MRTD holder in digital form.
Digital Signature Algorithm (DSA)	Asymmetric algorithm published by NIST in FIPS 186. This algorithm only provides digital signature function.
Digital (cryptographic) Signature Scheme	A tuple of three algorithms. The key-generation algorithm takes as input a security parameter and outputs a key pair consisting of a private and a public key. The signature algorithm takes as input a private key, and a message, and outputs a cryptographic signature. The verification algorithm takes as input a public key, a message, and a signature, and outputs “valid” if the signature was generated using the signature generation algorithm with the private key of the key pair and the message as input, and “invalid” otherwise.
(Digital) Document Feature	A property of a document which can be used to verify the contents of the document. Examples are textual information such as the name of the holder, or the issuing date, or a printed image of the document holder. A digital document feature is the digitized version of a document feature.
Digital Seal	Short for Visible Digital Seal.
Digital Travel Authorization	An electronic visa, issued and maintained within the issuing state.
Digital Watermark	See: Steganography.
Directory/Public Key Directory (PKD)	A repository for storing information. Typically, a directory for a particular PKI is a repository for the public key encryption certificates issued by that PKI’s Certification Authority, along with other client information. The directory also keeps cross-certificates, Certification Revocation Lists, and Authority Revocation Lists.
Displayed signature	The original written signature or the digitally printed reproduction of the original.
Document blanks	A document blank is a travel document that does not contain personalized data. Typically, document blanks are the base stock from which personalized travel documents are created.
Document model	Covers the document series of a nation, which have the same optical appearance (e.g. (D, P, 1, 2005), (D, P, 2, 2007) and (D, P, 3, 2010). One nation can have multiple valid document models in circulation at a given time (e.g. (GBR, P, 1, 2008) and (GBR, P, 2, 2010).
Document number	A number that uniquely identifies a document. It is recommended that the document number and the control number be identical.

Term	Definition
Document signer	A body which issues a biometric document and certifies that the data stored on the document is genuine in a way that will enable detection of fraudulent alteration.
Duplex design	A design made up of an interlocking pattern of small irregular shapes, printed in two or more colours and requiring very close register printing in order to preserve the integrity of the image.
Eavesdropping	The unauthorized interception of data communication.
Effective reading zone (ERZ)	A fixed-dimensional area, common to all MRTDs, in which the machine readable data in the MRZ can be read by document readers.
Electrically Erasable Programmable Read Only Memory (EEPROM)	A non-volatile memory technology where data can be electrically erased and rewritten.
Electronic Machine Readable Passport (eMRP)	A TD3 size MRTD conforming to the specifications of Doc 9303-4, that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the holder. Commonly referred to as “ePassport”.
Electronic Machine Readable Travel Document (eMRTD)	An MRTD (passport, visa or card) that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant Part of Doc 9303 — *Machine Readable Travel Documents*.
Electronic MROTD	A TD1 or TD2 size MROTD conforming to the specifications of Doc 9303-5 or Doc 9303-6, respectively, that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the holder.
Embedded image	An image or information encoded or concealed within a primary visual image. Also see steganography.
Encryption	The act of disguising information through the use of a key so that it cannot be understood by an unauthorized person.
End user	A person who interacts with a biometric system to enroll or have his[1] identity checked.
Enrollee	A human being, i.e. natural person, assigned an MRTD by an issuing State or organization.
Enrollment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person’s identity.
ePassport	Commonly used name for an eMRP. See Electronic Machine Readable Passport (eMRP).
Extraction	The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
Exposure value	Number that represents a combination of a camera's shutter speed and f-number, such that all combinations that yield the same exposure have the same EV.

1. Throughout this document, the use of the male gender should be understood to include male and female persons.

Term	Definition
Eye centre	Centre of the line connecting the inner and the outer corner of the eye. Note 1: The eye centres are the feature points 12.1 and 12.2 as defined in ISO/IEC 14496-2. Note 2: The inner and the outer corner of the eye are defined by ISO/IEC 14496-2. They are the feature points 3.12 and 3.8 for the right eye, and 3.11 and 3.7 for the left eye.
Eye to mouth distance	Distance between the face centre M and the mouth midpoint (feature point 2.3 from ISO/IEC 14496-2).
Face centre	Midpoint of the line connecting the two eye centres.
Failure to acquire	The failure of a biometric system to obtain the necessary biometric to enroll a person.
Failure to enroll	The failure of a biometric system to enroll a person.
False Acceptance	When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
False Acceptance Rate (FAR)	The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as FAR = NFA/NIIA or FAR = NFA/NIVA where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts.
False match rate	Alternative to “false acceptance rate”; used to avoid confusion in applications that reject the claimant if his biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of “false acceptance” and “false rejection”.
False non-match rate	Alternative to “false rejection rate”; used to avoid confusion in applications that reject the claimant if his biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of “false acceptance” and “false rejection”.
False rejection	When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.
False rejection rate (FRR)	The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The false rejection rate may be estimated as follows: FRR = NFR/NEIA or FRR = NFR/NEVA where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrollee identification attempts, and NEVA is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of enrollees. The false rejection rate normally excludes “failure to acquire” errors.
Feature	An element of the document which is suitable for the proof of authenticity (e.g. IR-absorbent photo).
Fibres	Small, thread-like particles embedded in a substrate during manufacture.
Field	Specified space for an individual data element within a zone.
Fingerprint(s)	One (or more) visual representation(s) of the surface structure of the holder’s fingertip(s).

Term	Definition
Fluorescent ink	Ink containing material that glows when exposed to light at a specific wavelength, usually UV.
Forgery	Fraudulent alteration of any part of the genuine document.
Fraudulent Alteration	Involves the alteration of a genuine document in an attempt to enable it to be used for travel by an unauthorized person or to an unauthorized destination. The biographical details of the genuine holder, particularly the portrait, form the prime target for such alteration.
Front-to-back (see-through) register	A design printed on both sides of an inner page of the document which, when the page is viewed by transmitted light, forms an interlocking image.
Full frontal (facial) image	A portrait of the holder of the MRTD produced in accordance with the specifications established in Doc 9303.
Full size (Format-A) machine readable visa (MRV-A)	An MRV conforming with the dimensional specifications contained in Doc 9303-7, sized to completely fill a passport visa page.
Gallery	The database of biometric templates of persons previously enrolled, which may be searched to find a probe.
Ghost Image	See: Shadow Image.
Global interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all eMRTDs.
Globally Interoperable Biometric	Refers to Face Image as set forth in Doc 9303-9.
Guilloche design	A pattern of continuous fine lines, usually computer generated, and forming a unique image that can only be accurately re-originated by access to the equipment, software and parameters used in creating the original design.
Hash	A mathematical formula that converts a message of any length into a unique fixed-length string of digits known as “message digest” that represents the original message. A hash is a one-way function, that is, it is infeasible to reverse the process to determine the original message. Also, a hash function will not produce the same message digest from two different inputs.
Heat-sealed laminate	A laminate designed to be bonded to the biographical data page of a passport book by the application of heat and pressure.
Holder	A person possessing an MRTD, submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity. A person who interacts with a biometric system to enroll or have his identity checked.
ICAO Public Key	The central database serving as the repository of Document Signer Certificates, CSCA

Term	Definition
Directory	Master Lists, Country Signing CA Link Certificates and Certificate Revocation Lists issued by Participants, together with a system for their distribution worldwide, maintained by ICAO on behalf of Participants in order to facilitate the validation of data in eMRTDs.
Identification/Identify	The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the eMRTD holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with “Verification”.
Identification card (ID-card)	A card used as an identity document.
Identifier	A unique data string used as a key in the biometric system to name a person’s identity and its associated attributes. An example of an identifier would be an MRTD number.
Identity	The collective set of distinct personal and physical features, data and qualities that enable a person to be definitively identified from others. In a biometric system, identity is typically established when the person is registered in the system through the use of so-called “breeder documents” such as birth certificate and citizenship certificate.
Identity Document	Document used to identify its holder and issuer, which may carry data required as input for the intended use of the document.
Image	A representation of a biometric as typically captured via a video, camera or scanning device. For biometric purposes this is stored in digital form.
Impostor	A person who applies for and obtains a document by assuming a false identity, or a person who alters his physical appearance to represent himself as another person for the purpose of using that person’s document.
Index marks	These marks are printed on the outside edge of each page in consecutive order starting from the top on the first page to a lower position on the following page and so on. The register mark of the last page appears at the bottom. This printing method leads to the appearance of a continuous stripe on the edge of the passport. Any page that has been removed will register as a gap. When printed in UV colour, this stripe becomes visible only under UV light. Also called collation marks.
Infra-red drop-out ink	An ink which forms a visible image when illuminated with light in the visible part of the spectrum and which cannot be detected in the infrared region.
Infra-red ink	An ink which is visible in the infrared light spectrum.
Initialization (of a smart card)	The process of populating persistent memory (EEPROM, etc.) with data that are common to a large number of cards while also including a minimal amount of card unique items (e.g. ICC serial number and Personalization keys).
Inspection	The act of a State or organization examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity.
Inspection system	A system used for inspecting MRTDs by any public or private entity having the need to validate the MRTD, and using this document for identity verification, e.g. border control authorities, airlines and other transport operators, financial institutions.

Term	Definition
Intaglio	A printing process used in the production of security documents in which high printing pressure and special inks are used to create a relief image with tactile feel on the surface of the document.
Integrated Circuit (IC)	Electronic component designed to perform processing and/or memory functions.
Integrated Circuit Card (IC card, ICC)	A card into which one or more ICs have been inserted,
Integrity	The ability to confirm that the Logical Data Structure and its components have not been altered from those created by the issuing State or organization.
Inter eye distance	Length of the line connecting the eye centres of the left and right eye.
Interface	A standardized technical definition of the connection between two components.
Interface device	Any terminal, communication device or machine to which the ICC is connected during operation.
Interoperability	The ability of several independent systems or sub-system components to work together.
Iris (printing)	See: Rainbow Printing.
Issuer	Organization that issues MRTDs.
Issuer data block	A series of Data Groups that are written to the optional capacity expansion technology by the issuing State or organization.
Issuing authority	The entity accredited for the issuance of an MRTD to the rightful holder.
Issuing State	The country issuing the MRTD.
Issuing organization	Organization authorized to issue an official MRTD (e.g. the United Nations Organization, issuer of the laissez-passer).
JPEG and JPEG2000	Standards for the data compression of images, used particularly in the storage of facial images.
Key exchange	The process for getting session keys into the hands of the conversants.
Key management	The process by which cryptographic keys are provided for use between authorized communicating parties.
Key pair	A pair of digital keys — one public and one private — used for encrypting and signing digital information.
Label	A self-adhesive sticker which is used as the data page within the passport. This is not a generally recommended practice, particularly for longer-term validity documents.
Laissez-passer	A document, generally similar to a passport, issued under the auspices of a supranational entity (e.g. United Nations).
Laminate	A clear material, which may have security features designed to be securely bonded to protect the biographical data or other page of the document.
Laser engraving	A process whereby personalized data are “burned” into the substrate with a laser. The

Term	Definition
	data may consist of text, portraits and other security features.
Laser perforation	A process whereby numbers, letters or images are created by perforating the substrate with a laser.
Latent image	A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles, achieved by intaglio printing.
Lenticular Feature	Security feature in which a lens structure is integrated in the surface of the document or used as a verification device.
Level 1 inspection	Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features).
Level 2 inspection	Examination by trained inspectors with simple equipment.
Level 3 inspection	Inspection by forensic specialists.
Live capture	The process of capturing a biometric sample by an interaction between an MRTD holder and a biometric system.
Locked (chip)	After personalization the chip MUST be locked. This means that no personalization commands can be executed anymore, and no personalization data can be written to the chip. Only after successful execution of an authentication mechanism (TA) data can be written to the chip. A locked chip cannot be ‘unlocked’.
Logical Data Structure (LDS)	The Logical Data Structure describes how data are stored and formatted in the contactless IC of an eMRTD.
Machine Assisted Document Verification	A process using a device to assist in the verification of the authenticity of the document in respect to data and/or security.
Machine Readable Official Travel Document (MROTD)	A document, usually in the form of a card of TD1 or TD2 size, that conforms to the specifications of Doc 9303-5 and Doc 9303-6 and may be used to cross international borders by agreement between the States involved.
Machine Readable Passport (MRP)	A passport conforming with the specifications contained in Doc 9303-4. Normally constructed as a TD3 size book containing pages with information on the holder and the issuing State or organization and pages for visas and other endorsements. Machine readable information is contained in two lines of OCR-B text, each with 44 characters.
Machine Readable Travel Document (MRTD)	Official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel (e.g. MRP, MRV, MROTD) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine.
Machine Readable Visa (MRV)	A visa conforming with the specifications contained in Doc 9303-7. The MRV is normally attached to a visa page in a passport.
Machine Readable Zone (MRZ)	Fixed dimensional area located on the MRTD, containing mandatory and optional data formatted for machine reading using OCR methods.
Machine-verifiable	A unique physical personal identification feature (e.g. facial image, fingerprint or iris) stored

Term	Definition
biometric feature	electronically in the chip of an eMRTD.
Magnification distortion	Image imperfection where the degree of magnification varies with the distance from the camera and the depth of the face.
Master key	Root of the derivation chain for keys.
Master List	A Master List is a digitally signed list of CSCA certificates that are 'trusted' by the Receiving State that issued the Master List (see Doc 9303-12).
Master List Signer	An entity that digitally signs a Master List of CSCA certificates. The Master List signer is authorized by its national CSCA to perform this function through the issuance of a Master List Signer certificate.
Match/Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. A decision to accept or reject is then based upon whether this score exceeds the given threshold.
Message	The smallest meaningful collection of information transmitted from sender to receiver. This information may consist of one or more card transactions or card transaction-related information.
Message Authentication Code (MAC)	A MAC is a message digest appended to the message itself. The MAC cannot be computed or verified unless a secret is known. It is appended by the sender and verified by the receiver which is able to detect a message falsification.
Metallic ink	Ink exhibiting a metallic-like appearance.
Metameric inks	A pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a mismatch at other wavelengths.
Microprint	Printed text or symbols smaller than 0.25 mm/0.7 pica points.
Moiré pattern	Artefact resembling a wavy pattern caused by photographing a scene or object containing repetitive details (e.g., lines, dots, etc.) that exceed the sensor resolution of the camera.
Morphing	Image manipulation technique where two or more subjects' faces are morphed or blended together to form a single face in a photograph.
MP	Measurement Pattern side length: the intensity measurement zones have a square shape and a size of 30% inter eye distance; they are used for measuring the lighting intensity on cheeks, forehead, and chin.
MRP data page	A fixed-dimensional page within the MRP containing a standardized presentation of visual and machine readable data.
Multiple biometric	The use of more than one biometric.
Non-volatile memory	A semiconductor memory that retains its content when power is removed (i.e. ROM, EEPROM).
One-to-a-few	A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a "watch list" of persons who warrant detailed identity investigation or are known criminals,

Term	Definition
	terrorists, etc.
One-to-many	Synonym for “Identification”.
One-to-one	Synonym for “Verification”.
Operating system	A programme which manages the various application programmes used by a computer.
Optically Variable Device (OVD)	Security Feature displaying different colours or image appearance depending on viewing angle or verification conditions.
Optically Variable Feature (OVF)	An image or feature whose appearance in colour and/or design changes dependent upon the angle of viewing or illumination. Examples are: features including diffraction structures with high resolution (diffractive optically variable image device/DOVID), holograms, colour-shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.
Out-of-band	Refers to communications which occur outside of a previously established communication method or channel.
Overlay	An ultra-thin film or protective coating that may be applied to the surface of a document in place of a laminate.
Padding	Appending extra bits to either side of a data string up to a predefined length.
Parallax	Displacement or difference in the apparent position of an object viewed along two different lines of sight, measured by the angle or semi-angle of inclination between those two lines.
Penetrating numbering ink	Ink containing a coloured component, which penetrates deep into a substrate.
Personal Identification Number (PIN)	A numeric security code used as a mechanism for local one-to-one verification with the purpose to ascertain whether the card holder is in fact the natural person authorized to access or use a specific service such as the right to unlock certain information on the card.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
Phosphorescent ink	Ink containing a pigment that glows when exposed to light of a specific wavelength, the reactive glow remaining visible and then decaying after the light source is removed.
Photo booth	Automated system for digitally capturing identity photographs in either public or office environments; it encloses the subject in a highly-controlled lighting environment and consists of a camera, lighting and peripheral devices such as printers; it has entrances on one or both sides with reflective curtains protecting against ambient light.
Photochromic ink	An ink that undergoes a reversible colour change when exposed to light of a specified wavelength.
Photo kiosk	Semi-automated system for digitally capturing identity photographs in a bureau-environment; it consists of camera and lighting and usually has a separate panel placed behind the subject to provide the required background but is otherwise open.
Photo-substitution	A type of forgery in which the portrait in a document is substituted for a different one after the document has been issued.

Term	Definition
Physical security	The range of security measures applied during production and personalization to prevent theft and unauthorized access to the process.
Physical visa	A foil type travel document placed within the traveller's passport.
PKD participant	An ICAO Member State or other entity issuing or intending to issue eMRTDs that follows the arrangements for participation in the ICAO PKD.
Portrait	A visual representation of the facial image of the holder of the MRTD in printed and electronically stored manner.
Presentation attack	Presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system.
Presentation attack detection	Automated determination of a presentation attack.
Private Key	The private component of an integrated asymmetric key pair (known only to the user), employed in public key cryptography in decrypting or signing information.
Probe	The biometric sample of the enrollee whose identity is sought to be established.
Public Key	The public component of an integrated asymmetric key pair, used in encrypting or verifying information.
Public key certificate	The public key information of an entity signed by the certification authority and thereby rendered unforgettable.
Public key cryptography	A form of asymmetric encryption where all parties possess a pair of keys, one private and one public, for use in encryption and digital signing of data.
Public Key Infrastructure (PKI)	A set of policies, processes and technologies used to verify, enrol and certify users of a security application. A PKI uses public key cryptography and key certification practices to secure communications.
Public key system	A cryptographic method using pairs of keys, one of which is private and one is public. If encipherment is done using the public key, decipherment requires application of the corresponding private key and vice versa.
Radial distortion	Image imperfection where the degree of magnification varies with the distance from the optical axis.
Rainbow printing (iris or split fountain printing)	A technique whereby two or more colours of ink are printed simultaneously on a press to create a continuous merging of the colours similar to the effect seen in a rainbow. Also called prismatic, or iris printing.
Random access	A means of storing data whereby specific items of data can be retrieved without the need to sequence through all the stored data.
Random Access Memory (RAM)	A volatile memory randomly accessible used in the IC that requires power to maintain data.
Reactive inks	Inks that contain security reagents to guard against attempts at tampering by chemical erasure (deletion), such that a detectable reaction occurs when bleach and solvents come into contact with the document.

Term	Definition
Read only memory (ROM)	Non-volatile memory that is written once, usually during IC production. It is used to store operating systems and algorithms employed by the semiconductor in an integrated circuit card during transactions.
Read range	The maximum practical distance between the contactless IC with its antenna and the reading device.
Receiver data block	A series of Data Groups that are written to the optional capacity expansion technology by a receiving State or authorized receiving organization.
Receiving State	The country inspecting the holder's MRTD.
Reference data set	The visual-, IR-, and UV-pictures of a reference document define the check routines for a corresponding document model.
Reference document set	The set of documents, whose reference data-sets are used to define check routines.
Registration	The process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.
Registration Authority (RA)	A person or organization responsible for the identification and authentication of an applicant for a digital certificate. An RA does not issue or sign certificates.
Relief (3-D) design (Medallion)	A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.
Response	A message returned by the slave to the master after the processing of a command received by the slave.
Rivest, Shamir and Adleman (RSA)	Asymmetric algorithm invented by Ron Rivest, Adi Shamir and Len Adleman. It is used in public-key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.
Score	A number on a scale from low to high, measuring the success that a biometric probe record (the person being searched for) matches a particular gallery record (a person previously enrolled).
Secure hash algorithm (SHA)	Hash function specified by NIST and published as a federal information processing standard FIPS-180.
Secured message	A message that is protected against illegal alteration or origination.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
Security thread	A thin strip of plastic or other material embedded or partially embedded in the substrate during the paper manufacturing process. The strip may be metallized or partially de-metallized.
See-through register (front-to-back)	See: front-to-back register.
Sensitive Data	These data are considered to be more privacy sensitive than non-sensitive data. Access to sensitive data SHOULD be more restricted. Doc 9303-11 specifies Terminal Authentication

Term	Definition
	as an interoperable mechanism for accessing sensitive data. If no interoperability is required, other mechanisms can be used.
Shadow Image	Used as a synonym to Ghost Image: A second representation of the holder's portrait on the document, reduced in contrast and/or saturation and/or size.
Sheet	The individual piece of substrate in a passport which comprises more than one passport page.
Size 1 machine readable official travel document (TD1)	A card with nominal dimensions guided by those specified for the ID-1 type card (ISO/IEC 7810) (excluding thickness).
Size 2 machine readable official travel document (TD2)	A card or label conforming with the dimensions defined for the ID-2 type card (ISO/IEC 7810) (excluding thickness).
Skimming	Electronically reading the data stored in the contactless IC without authorizing this reading of the document.
Small size (Format-B) machine readable visa (MRV-B)	An MRV conforming with the dimensional specifications contained in Doc 9303-7, sized to maintain a clear area on the passport visa page.
Spoofing	Faking the sending address of a transmission to gain illegal entry into a secure system. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.
Steganography	An image or information encoded or concealed within a primary visual image.
Structure feature	A structure feature involves the incorporation of a measurable structure into or onto the MRTD. The presence of the structure may be detected and measured by the detection machine.
Subject	Person which is to be displayed on the portrait, this person is intended to be the holder of the MRTD.
Substance feature	A substance feature involves the incorporation into the MRTD of a material which would not normally be present and is not obviously present on visual inspection. The presence of the material may be detected by the presence and magnitude of a suitable property of the added substance.
Symmetric algorithm	A type of cryptographic operation using the same key or set of keys for encryption of plain text and decryption of associated cipher text.
Synthetic	A non-paper based material used for the biographical data page or cards. The term "synthetic" is used synonymously for "plastic", which encompasses materials like polycarbonate, PET and similar materials and combinations thereof.
System	A specific IT installation, with a particular purpose and operational environment.
System integration	The process by which cardholder-facing, internal and partner-facing systems and applications are integrated with each other.

Term	Definition
System security policy	The set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system.
Tactile feature	A surface feature giving a distinctive “feel” to the document.
(Feature) Tag	A byte that uniquely identifies a document feature. The mapping between feature tags and features must be specified in a profile.
Taggant	A not-naturally occurring substance that can be added to the physical components of an MRTD, and is typically a Level 3 feature, requiring special equipment for detection.
Tagged ink	Inks containing compounds that are not naturally occurring substances and which can be detected using special equipment.
Tamper resistance	The capability of components within a document to withstand alteration.
Template/Reference template	Data which represent the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.
Template size	The amount of computer memory taken up by the biometric data.
Thermochromic ink	An ink which undergoes a reversible colour change when the printed image is exposed to a specific change in temperature.
Threshold	A “benchmark” score. The comparison of the result value of a check routine to a corresponding threshold leads to a Passed-/Failed-decision.
Trust Anchor	In cryptographic systems with hierarchical structure this is an authoritative entity for which trust is assumed and not derived.
Token image	A portrait of the holder of the MRTD, typically a full frontal image, which has been adjusted in size to ensure a fixed distance between the eyes. It may also have been slightly rotated to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the portrait rectangle if this has not been achieved when the original portrait was taken or captured.
Usual Mark	Symbol that replaces a holder’s written signature in case the holder is not able to sign.
UV dull substrate	A substrate that exhibits no visibly detectable fluorescence when illuminated with UV light.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Variable laser image	A feature generated by laser engraving or laser perforation displaying changing information or images dependent upon the viewing angle.
Verification/verify	Biometrics: The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee’s template. Contrast with “Identification”. Machine Authentication: A verification describes the application of a check routine to a live data-set of a document model. The result of a verification is mostly provided by a numeric result value.

Term	Definition
Visa Signer (VS)	The authority that receives data from a visa personalization system and that uses a VS certificate and the corresponding private key to encode and sign a visible digital seal.
Visa Signer Certificate	A certificate containing information identifying the entity that signed a visible digital seal on a visa, and containing the public key corresponding to the private key with which the signature was created.
Visa Validation Authority (VVA)	The authority that validates a visible digital seal based on a visa based on a validation policy.
Visible Digital Seal (VDS)	A cryptographically signed data structure containing document features, encoded as a 2D bar code and printed on a document.
Visual inspection zone (VIZ)	Those portions of the MRTD (data page in the case of MRP) designed for visual inspection, i.e. front and back (where applicable), not defined as the MRZ.
Watermark	A custom design, typically containing tonal gradation, formed in the paper or other substrate during its manufacture, created by the displacement of materials therein, and traditionally viewable by transmitted light.
Wavelet Scalar Quantization (WSQ)	A means of compressing data used particularly in relation to the storage of fingerprint images.
Windowed or Transparent feature	Security feature created by the construction of the substrate, whereby part of the substrate is removed or replaced by transparent material, which can incorporate additional security features such as lenses or tactile elements.
X.509 v3 certificate	The internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, user's identifying information, and issuer's digital signature.
Zone	An area containing a logical grouping of data elements on the MRTD. Seven (7) zones are defined for MRTDs.

4.3 Key Words

Key words are used to signify requirements.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in capitalized form in Doc 9303 are to be interpreted as described in [RFC 2119]:

MUST	This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT	This phrase, or the phrase “NOT RECOMMENDED” means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that an item is truly optional. One user may choose to include the item because a particular application requires it or because the user feels that it enhances the application while another user may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).
CONDITIONAL	The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED. This is an additional key word used in Doc 9303 (not part of RFC 2119).

Guidance in the use. Imperatives of the type defined here must be used with care and sparingly. In particular, they MUST be used only where it is actually required for interoperation or to limit behaviour which has potential for causing harm (e.g. limiting retransmissions). For example, they must not be used to try to impose a particular method on implementers where the method is not required for interoperability.

Security considerations. These terms are frequently used to specify behaviour with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done, may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementers will not have had the benefit of the experience and discussion that produced the specification.

In case OPTIONAL features are implemented, they MUST be implemented as described in Doc 9303.
In Doc 9303, Appendices are informative. If one claims compliancy to an (informative) appendix, the key words used in that appendix MUST be respected as specified here.

4.4 Object Identifiers

In Parts 9303-3, 9303-10, 9303-11, and 9303-12 ICAO Object Identifiers are specified. This paragraph lists these actual ICAO Object Identifiers:

```
-- ICAO security framework
id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}


-- LDS security object
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 1}
```

```
-- CSCA master list
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 2}

id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 3}


-- Active Authentication protocol
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 5}


-- CSCA name change
id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security
6}

id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-
mrtd-security-extensions 1}


-- document type list, see TR "LDS and PKI Maintenance"
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-
icao-mrtd-security-extensions 2}


-- Deviation List Base Object identifiers
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 7}

id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 8}


id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 2}

id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-
Deviation-CertOrKey 4}

id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}

id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS
3}
```

```
id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}


-- LDS2 Object Identifiers
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}

id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}

id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}

id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}

id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 1}

id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 3}

id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}

id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
visaRecords 1}

id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-visaRecords
3}

id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}

id-icao-lds2- additionalBiometrics-application OBJECT IDENTIFIER ::= { id-icao-
lds2- additionalBiometrics 1}

id-icao-lds2- additionalBiometrics-access OBJECT IDENTIFIER ::= { id-icao-lds2-
additionalBiometrics 3}


-- SPOC Object Identifiers
id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}

id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}
```

```
id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}


-- VDS Object Identifiers
id-icao-vds OBJECT IDENTIFIER ::= { id-icao-mrtd-security 11}


-- DTC Object Identifiers
id-icao-dtc OBJECT IDENTIFIER ::= { id-icao-mrtd-security 12}

id-icao-dtcSigner OBJECT IDENTIFIER ::= {id-icao-dtc 1}

id-icao-dtcAttributes OBJECT IDENTIFIER ::= {id-icao-dtc 2}

id-icao-dtcCapabilitiesInfo OBJECT IDENTIFIER ::= {id-icao-dtcAttributes 1}


-- EF.DIR Object Identifiers
id-EFDIR OBJECT IDENTIFIER ::= { id-icao-mrtd-security 13}
```

4.5 The Use of Notes

While in ISO/IEC standards notes are informative, in Doc 9303 notes are part of the normative text and used to emphasize requirements or additional information.

5. GUIDANCE ON THE USE OF DOC 9303

5.1 Doc 9303 Composition

Doc 9303 is comprised of thirteen parts. Each part describes a specific aspect of the MRTD. The parts of Doc 9303 are composed in such way that the issuer of MRTDs can compose a complete set of relevant specifications, relevant to a specific type of MRTD (form factor). The relationship between these form factors and the parts of Doc 9303 is described in Section 5.2 of this Part 1.

The following parts form the complete Doc 9303 specifications for Machine Readable Travel Documents:

Part 1 — Introduction
The document at hand is Part 1.

Part 2 — Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
Part 2 provides mandatory and optional specifications for the precautions to be taken by travel document issuing authorities to ensure that their MRTDs, and their means of personalization and issuance to the rightful holders, are secure against fraudulent attack. Mandatory and optional specifications are also provided for the physical security to be provided at the premises where the MRTDs are produced, personalized and issued and for the vetting of personnel involved in these operations.

Part 3 — Specifications common to all MRTDs
Part 3 defines specifications that are common to TD1, TD2 and TD3 size Machine Readable Travel Documents (MRTDs) including those necessary for global interoperability using visual inspection and machine readable (optical character recognition) means. Detailed specifications applicable to each document type appear in Doc 9303, Parts 4 through 7.

Part 4 — Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs
Part 4 defines specifications that are specific to TD3 size Machine Readable Passports (MRPs) and other TD3 size Machine Readable Travel Documents (MRTDs). For brevity, the term MRP has been used throughout Part 4 and, except where stated, all the specifications herein shall apply equally to all other TD3 size MRTDs.

Part 5 — Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs)
Part 5 defines specifications that are specific to TD1 size Machine Readable Official Travel Documents (MROTDs).

Part 6 — Specifications for TD2 size Machine Readable Official Travel Documents (MROTDs)
Part 6 defines specifications that are specific to TD2 size Machine Readable Official Travel Documents (MROTDs).

Part 7 — Machine Readable Visas
Part 7 defines the specifications for Machine Readable Visas (MRVs) which allow compatibility and global interchange using both visual (eye readable) and machine readable means. The specifications for visas can, where issued by a State and accepted by a receiving State, be used for travel purposes. The MRV shall, as a minimum, contain the data specified in a form that is legible both visually and by optical character recognition methods, as presented in Part 7.

Part 7 contains specifications for both Format-A as well as Format-B types of visas, and is based on the Third Edition of Doc 9303, Part 2, *Machine Readable Visas* (2005).

Part 8 — Emergency Travel Documents
Part 8 provides guidance and specifications on Emergency Travel Documents (ETDs). The purpose of this guidance material is to promote a consistent approach in the issuance of ETDs in order to enhance the security of the document, protect the individual, promote greater confidence for border staff in handling ETDs at ports, and address the vulnerabilities presented by inconsistent practices and security features. Part 8 also specifies the use of Visible Digital Seals in ETDs.

Part 9 —Deployment of Biometric Identification and Electronic Storage of Data in MRTDs
Part 9 defines the specifications, additional to those for the basic MRTD set forth in Parts 3, 4, 5, 6, and 7 of Doc 9303, to be used by States wishing to issue an electronic Machine Readable Travel Document (eMRTD) capable of being used by any suitably equipped receiving State to read from the document a greatly increased amount of data relating to the eMRTD itself and its holder. This includes mandatory globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems. The specifications require the globally interoperable biometric data to be stored in the form of high-resolution images.

Part 10 — Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)
Part 10 defines a Logical Data Structure (LDS) for eMRTDs required for global interoperability. The contactless integrated circuit capacity expansion technology contained in an eMRTD selected by an issuing State or organization SHALL allow data to be accessible by receiving States. Part 10 defines the specifications for the standardized organization of these data. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that SHALL be followed to achieve global interoperability for reading of details (Data Elements) recorded in the capacity expansion technology optionally included on an MRTD (eMRTD).

Part 11 — Security Mechanisms for MRTDs
Part 11 provides specifications to enable States and suppliers to implement cryptographic security features for Machine Readable Travel Documents (eMRTDs) offering ICC read-only access.

Part 11 specifies cryptographic protocols to:

- prevent skimming of data from the contactless IC;
- prevent eavesdropping on the communication between the IC and reader;
- provide authentication of the data stored on the IC based on the PKI described in Part 12, and provide authentication of the IC itself.

Part 12 — Public Key Infrastructure for MRTDs
Part 12 defines the Public Key Infrastructure (PKI) for the eMRTD application. Requirements for issuing States or organizations are specified, including operation of a Certification Authority (CA) that issues certificates and CRLs. Requirements for receiving States and their Inspection Systems validating those certificates and CRLs are also specified.

Part 13 — Visible Digital Seals for non-electronic documents
Part 13 specifies a digital seal to ensure the authenticity and integrity of non-electronic documents in a comparatively cheap, but highly secure manner using asymmetric cryptography. The information on the non-electronic document is cryptographically signed, and the signature is encoded as a two-dimensional bar code and printed on the document itself.

5.2 Relationship between MRTD Form Factors and relevant Doc 9303 Parts

Table 1-1 describes which parts of Doc 9303 are relevant for specific types of MRTDs (form factors).

Table 1-1. Form factors cross-reference table

	Doc 9303 Part												
	1	2	3	4	5	6	7	8	9	10	11	12	13
TD3 size MRTD (MRP)	√	√	√	√									
TD3 size eMRTD (eMRP)	√	√	√	√					√	√	√	√	

TD1 size MROTD	√	√	√		√								
TD1 size eMROTD	√	√	√		√				√	√	√	√	
TD2 size MROTD	√	√	√			√							
TD2 size eMROTD	√	√	√			√			√	√	√	√	
MRV	√	√	√				√						√
ETD	√	√	√					√					√

6. REFERENCES (NORMATIVE)

Certain provisions of international Standards, referenced in this text, constitute provisions of Doc 9303. Where differences exist between the specifications contained in Doc 9303 and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, including machine readable visas, the specifications contained herein shall prevail.

Annex 9 Convention on International Civil Aviation (“Chicago Convention”), Annex 9 – *Facilitation.*

RFC 2119 RFC 2119, S. Bradner, “Key Words for Use in RFCs to Indicate Requirement Levels”, BCP 14, RFC2119, March 1997.

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eight Edition, 202X

Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*
ISBN 978-92-9249-791-0

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

Page

1. SCOPE

This Part provides mandatory and optional specifications for the precautions to be taken by travel document issuing authorities to ensure that their MRTDs, and their means of personalization and issuance to the rightful holders, are secure against fraudulent attack. Mandatory and optional specifications are also provided for the physical security to be provided at the premises where the MRTDs are produced, personalized and issued and for the vetting of personnel involved in these operations.

The worldwide increase in the number of people travelling and the expected continued growth, together with the growth in international crime, terrorism and illegal immigration have led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse. Historically, Doc 9303 has not made recommendations on the specific security features to be incorporated in travel documents. Each issuing State has been free to incorporate such safeguards as it deemed appropriate to protect its nationally issued travel documents against counterfeiting, forgery and other forms of attack, as long as nothing was included which would adversely affect their OCR machine readability.

To meet the need of increased document security, ICAO's technical advisors decided it would be desirable to publish a set of "recommended minimum security standards" as a guideline for all States issuing machine readable travel documents. Thus,

- Appendix A to this Part describes security measures to be taken within the structure of the MRTD and of the premises in which it is produced;
- Appendix B describes optional means of achieving Optical Machine Authentication;
- Appendix C describes the security measures to be taken to ensure the security of the personalization operations and of the documents in transit.

2. SECURITY OF THE MRTD AND ITS ISSUANCE

Before the issuance of a travel document, the establishment of the holder and the entitlement to a travel document shall be carried out in line with the [ICAO EOI], ICAO TRIP Guide on Evidence of Identity, available at https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

The MRTD, and its method of issuance, shall be designed to incorporate safeguards to protect the document against fraudulent attack during its validity period. Methods of fraudulent attack can be classified as follows:

- *Counterfeit* involves the creation of all or part of a document which resembles the genuine MRTD with the intention that it be used as if it were genuine. Counterfeits may be produced by attempting to duplicate or simulate the genuine method of manufacture and the materials used therein or by using copying techniques;
- *Fraudulent alteration, also known as forgery*, involves the alteration of a genuine document in an attempt to enable it to be used for travel by an unauthorized person or to an unauthorized destination. The biographical details of the genuine holder, particularly the portrait, form the prime target for such alteration; and

- *Impostors*. "Impostor" is defined as someone representing himself[1] to be some other person. Security features should be incorporated to facilitate the visual and/or automated detection of fraudulent use of the MRTD by an impostor.

  Spoofing. Faking the sending address of a transmission to gain illegal entry into a secure system. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

- *Morphing*. Morphing is an image manipulation technique where two or more subjects' faces are morphed or blended together to form a single face in a photograph.

There are established methods of providing security against the above types of fraudulent attack. These involve the use of materials which are not readily available, combined with highly specialized design systems and manufacturing processes requiring special equipment and expertise. Appendix A to this Part lists some of the techniques currently known to be available to provide security to an MRTD enabling an inspecting officer to detect a counterfeit or fraudulently altered document either visually or with the aid of simple equipment such as a magnifying glass or ultraviolet lamp.

All MRTDs that conform to Doc 9303 shall use the specified Basic Security Features listed in Table 1 in Appendix A.

3. MACHINE ASSISTED DOCUMENT VERIFICATION

In the field of machine assisted authentication of Machine Readable Travel Documents (MRTDs), considerable progress has been made over the last decade. Technical innovations made in the security design of MRTDs and in the development of authentication systems (readers, software, etc.) have allowed for machine-based document authentication to become an integral part of several control infrastructures and processes (e.g. border control).

However, new challenges arise for document experts, manufacturers and authorities involved in the field as technical improvements achieve higher security and efficiency in operational processes. Some of the main challenges are the lack of harmonization and standardization of the processes in place, and the lack of coordination between the main parties involved in those processes, both leading to system parts and components being developed independently without consideration for major implications resulting from their interaction. Furthermore, the complexity and diversity of the systems currently available on the market make it especially difficult to evaluate and/or compare them.

This section provides advice on machine assisted authentication of security features incorporated in MRTDs made in accordance with the specifications set out in Doc 9303. While Appendix A of this Part and the security standards recommended therein provide the basis for the considerations in this section, Appendix B contains recommendations which cover machine verification of those security features (based on materials, on security printing and on copy protection techniques) using the capability of document readers for high resolution image acquisition in the visual, infrared and ultraviolet spectral range. Finally, Appendix C provides a set of best practice recommendations for the main parties involved in the design, implementation and operation of the machine authentication systems and key components.

The aim of the recommendations in this chapter is to improve the security of machine readable travel documents worldwide by using machine assisted document verification procedures completely in line with:

1 Throughout this document, the use of the male gender should be understood to include male and female persons.

- the layout of machine readable travel documents as specified in Doc 9303 maintaining backward compatibility;
- the security features recommended in Appendix A of this Part; and
- making use of the technical capabilities of advanced readers installed worldwide to accommodate eMRTDs as recommended in Appendix B and C of this Part.

However, each State must conduct a risk assessment of the machine assisted document authentication features at its borders to identify their most beneficial aspects and minimize the risks. Doc 9303 does not specify any feature as a means of globally interoperable machine assisted document verification, as the use of a single feature worldwide would make the feature highly vulnerable to fraudulent attack. Therefore, to minimize risk States should apply a variety of security features.

3.1 Feature Types

There are three main categories of machine-verifiable security features. These are described below along with examples of security features that are capable of machine verification.

3.1.1 Structure feature

A structure feature involves the incorporation of a measurable structure into or onto the MRTD data page. It is a security feature containing some form of verifiable information based on the physical construction of the feature. Examples include:

- the interference characteristic of a hologram or other optically variable device that can be uniquely identified by a suitable reader;
- retro-reflective images embedded within a security laminate; and
- controlled transmission of light through selective areas of the substrate.

3.1.2 Substance feature

A substance feature involves the incorporation into the MRTD of a material which would not normally be present and is not obviously present on visual inspection. The presence of the material may be detected by the presence and magnitude of a suitable property of the added substance. It involves the identification of a defined characteristic of a substance used in the construction of the feature. Examples include:

- the use of pigments, usually in inks, which respond in specific and unusual ways to specific wavelengths of light (which may include infrared or ultraviolet light) or have magnetic or electromagnetic properties; and
- the incorporation into a component of the data page of materials, e.g., fibres whose individual size or size distribution conform to a predetermined specification.

3.1.3 Data feature

The visible image of the MRTD data page may contain concealed information which may be detected by a suitable device built into the reader. The concealed information may be in the security printed data page but it is more usually incorporated into the personalization data especially the printed portrait.

Inserting the concealed information into the MRTD data page may involve the application of substance and/or structure features in a way which achieves several levels of security. The term steganography, in this context, describes a special class of data features typically taking the form of digital information which is concealed within an image, usually either the personalization portrait or the background security printing. The information may be decoded by a suitable device built into a full-page reader set to look for the feature in a specific location. The information might, for example, be the travel document number. The reader could then be programmed to compare the travel document number detected from the feature with the travel document number appearing in the MRZ. Such a comparison involves no access to any data stored in the contactless IC of an eMRTD. Examples of this type of feature are:

- encoded data stored on the document in magnetic media such as special security threads; and
- designs incorporating the concealed data which only become detectable when viewed using a specific wavelength of light, optical filters, or a specific image processing software.

In more complex forms the amount of stored data can be significant, and this can be verified by electronic comparison with data stored in the contactless IC of the eMRTD.

3.2 Basic Principles

All three feature types, namely structure, substance and data, may be incorporated in travel documents and verified using suitably designed readers. Readers are now becoming available that can detect such features and use the responses to confirm the authenticity of the document. Appendix B concentrates on features that can be verified by detection equipment built into the MRTD reader, and used during the normal reading process.

Machine assisted document security verification uses automated inspection technology to assist in verifying the authenticity of a travel document. It should not be used in isolation to determine proof of authenticity, but when used in combination with visible document security features the technology provides the examiner with a powerful new tool to assist in verifying travel documents.

Machine assisted document security verification features are optional security elements that may be included on the MRTD at the discretion of the issuing authority.

The machine verifiable security features may vary in size from less than 1 mm (0.04 in) square up to the whole area of the document. Figure 1 provides guidance on the positions these features should occupy on a MRTD data page to facilitate interoperability. To maintain backward compatibility, it is recommended to deploy machine authentication features within the positions and areas indicated.

3.3 Machine Authentication and eMRTDs

The use of a fully compliant, contactless IC in an eMRTD offers excellent possibilities for machine authentication. However, machine authentication using the contactless IC fails if:

- the contactless IC is defective and fails to communicate; or
- there are no certificates available for checking the authenticity and integrity of the data on the contactless

IC.

Therefore an alternative machine authentication is needed. This is especially relevant in automated border control (ABC) scenarios where the document reader is used instead of a border official to read and validate the eMRTD. As a reliable alternative, optical machine authentication establishes trust in the data used for decisions at the border.

A functioning contactless IC in an eMRTD can also aid optical machine authentication by storing the optical machine authentication features and its coordinates in the relevant Data Groups (DGs).

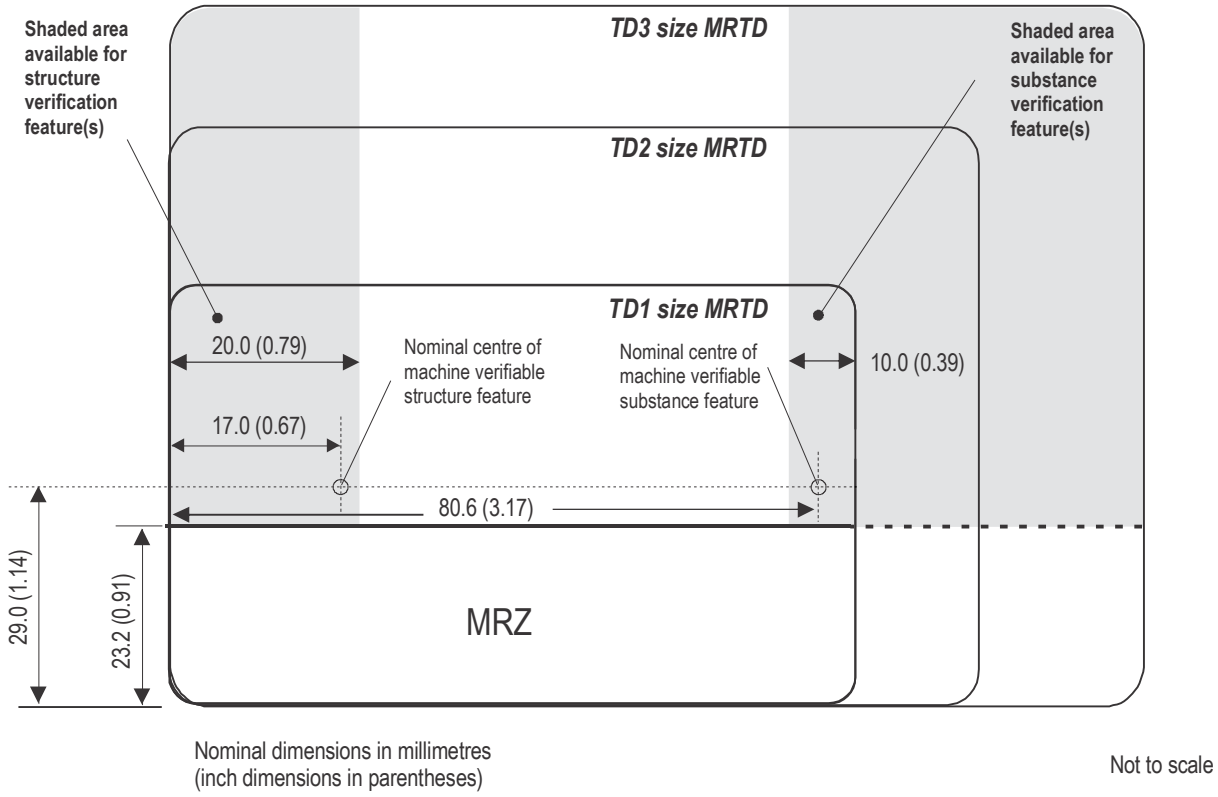


Figure 1. Three sizes of MRTD including the MRP (TD3 size) with recommended positions for machine assisted document verification features. The shaded area on the left is recommended for the incorporation of a structure feature and that on the right for the incorporation of a substance feature.

4. SECURITY OF MRTD PRODUCTION (DESIGN AND MANUFACTURING) AND ISSUANCE FACILITIES

The State issuing the MRTD shall ensure that the premises in which the MRTD is printed, bound, personalized and issued are appropriately secure and that staff employed therein have an appropriate security clearance. Appropriate security shall also be provided for MRTDs in transit between facilities and from the facility to the MRTD's holder. Appendix C provides recommendations as to how these requirements can be met.

The following factors should be considered in the establishment of production and issuance facilities:

1) resilience;

2) physical security and access control;

3) production materials and MRTD accounting;

4) transport;

5) personnel; and

6) cyber security.

4.1 Resilience

States should take adequate steps to ensure that MRTD production can be maintained in the event of disaster situations such as flood, fire and equipment failure. Some considerations are:

- use of distributed production and issuing facilities;
- secondary production sites when production is centralized;
- emergency issuing facilities;
- rapid access to spare parts and support;
- second sourcing of all MRTD components.

States are recommended to consider possible failure modes in the design of production and issuance facilities, with the objective of eliminating common failures and single-points of failure.

4.2 Physical Security and Access Control

States should control access to production and issuance facilities. Control should be zoned and the requirements for access to each zone should be commensurate with value of the assets being protected.

Some examples of good practice for production facilities are:

- wire cages or solid walls to segregate production areas;
- strong rooms for storage of finished, un-personalized MRTDs and key security components for MRTD production;
- security pass-based access control between zones;
- video surveillance inside and outside the facility;
- perimeter security;
- full-time security personnel.

States should also consider the security that is in place at organizations providing MRTD components to the production facility because theft or sale of such components could make it easier to forge an MRTD.

Issuance facilities should separate back-office areas from public areas, with access control between the two. Staff should be afforded adequate protection, as determined by local circumstance.

4.3 Production Material Accounting

States should ensure that all material used in the production of MRTDs is accounted for and that MRTD production is reconciled with MRTD orders, so that it may be demonstrated that no MRTDs or MRTD components are missing.

Defective materials, MRTDs and MRTD components should be securely destroyed and accounted for.

Generally, reducing the number of issuance and production sites will make material accounting easier. However, this must be balanced against the need to provide resilience and acceptable customer service.

4.4 Transport

States are advised to use secure methods to transport MRTDs and MRTD components; cash-in-transit methods are normally adequate unless particularly high-value assets are being transported (e.g. holographic masters).

States should seek to minimize the amount of material transported in any one batch to reduce the effect of theft. In particular, States should not transport complete sets of printing plates in one operation.

4.5 Personnel

States should ensure that all personnel are subject to a security clearance process, which confirms their identity and suitability for employment in an environment where high-value assets are produced. Staff should be provided with credentials to enable them to identify themselves and to gain access to secure areas which they need to access in connection with their role.

4.6 Cyber Security

Production and issuance facilities are vulnerable to a variety of cyber attacks, such as:

1) viruses and other malware, both in conventional computing facilities and in production machinery;

2) denial-of-service attacks through online MRTD application channels and web services exposed by production and issuance systems;

3) compromise of issuing systems to enable attackers to issue passports or steal personal data or cryptographic assets (such as private keys for eMRTD production).

Countermeasures for these and related attacks are beyond the scope of this document. States should seek advice from their national technical authority.

5. PROVISION OF INFORMATION ON NEWLY ISSUED MRTDS

It is recommended that a State launching a new design of MRTD inform all other States of the details of the new MRTD including evident security features, preferably providing personalized specimens for use as a reference by the receiving State's department which is responsible for verifying the authenticity of such documents. The distribution of such specimens should be made to established contact points agreed by the receiving States.

6. PROVISION OF INFORMATION ON LOST AND STOLEN MRTDS

The exchange of information on lost, stolen or revoked travel documents is a key strategy to strengthen border control and mitigate the impacts of identity theft and immigration fraud. Accordingly, States should consider implementing the following operational procedures to offset the threats that work to undermine border management and national public safety:

1. communicating proactively with document holders;

2. maintaining national databases of lost, stolen and revoked travel documents;

3. sharing information about lost, stolen and revoked travel documents with INTERPOL and verifying documents against INTERPOL databases systematically at primary inspection;

4. installing checks to determine whether a holder is presenting a lost, stolen or revoked document at a border crossing.

6.1 Communicating Proactively with Document Holders

States should ensure that holders of travel documents are fully aware of their responsibilities regarding the use, safe-keeping and reporting procedures for lost or stolen travel documents. Guidelines for safe-keeping travel documents both at home and while travelling may assist in preventing the loss or theft of travel documents. At the time holders receive their documents, holders should be informed of the appropriate actions (including timely reporting) and channels for reporting lost or stolen documents. To assist in this process, States may consider providing travel document holders with multiple channels for securely reporting lost and stolen documents, including in person, telephone, physical mail and various ways of electronic communication including Internet.

States must also take appropriate measures to ensure that holders of travel documents are educated about the potential disruptions, inconveniences and added expenses that can arise when lost, stolen or revoked documents are presented at border control for the purposes of travel. This advice should highlight that once a travel document has been reported lost/stolen it is cancelled and can no longer be used and may be seized by authorities if an attempt is made to use it.

National legislation, or any suitable framework, should be in place to oblige holders of travel documents to report a lost or stolen travel document immediately. No new travel document should be issued until this report has been filed.

6.2 Maintaining National Databases of Lost, Stolen and Revoked Travel Documents

States that use national travel document databases to assist in the verification of the status of their nationally-issued travel documents should take measures to ensure that information is kept up to date. Reports about lost and stolen documents provided by the holders should be recorded into these systems in a timely fashion to ensure that risk assessments conducted using these systems are accurate. States may also wish to consider recording information about lost, stolen or revoked travel documents intercepts in these databases. In addition to updating these databases, States should ensure that border control and police authorities are able to access them easily.

6.3 Sharing Information about Lost, Stolen and Revoked Travel Documents with INTERPOL and Verifying Documents against INTERPOL Databases Systematically at Primary Inspection

States should participate in the global interchange of timely and accurate information concerning the status of travel documents to support in-country policing and border management, as well as efforts to mitigate the impacts of identity theft. Sharing information about lost, stolen and revoked travel documents serves to:

a) improve the integrity of border management;

b) assist in detecting identity theft or immigration fraud at the border, or in other situations where the document is presented as a form of identification;

c) improve the chances of identifying terrorist operatives travelling on false documents;

d) improve the chances of identifying criminal activity, including people smuggling;

e) aid in the recovery of national documents; and

f) limit the value and use of lost, stolen or revoked documents for illegal purposes.

INTERPOL's Automated Search Facility (ASF)/Stolen and Lost Travel Document Database (SLTD) provides States with a means to effectively and efficiently share information about lost, stolen and revoked travel documents in a timely fashion. States should share information about lost and stolen documents that have been issued, as well as blank documents that have been stolen from a production or issuance facility or in transit. Appendix D outlines the factors that must be considered prior to participating in the ASF/SLTD.

States should verify documents against INTERPOL databases systematically at primary inspection to ensure that only travellers holding valid travel documents are crossing border control checkpoints. Verifying the status of travel documents against these databases offers many of the same benefits afforded by sharing information about lost, stolen and revoked documents.

6.4 Installing Checks to Determine Whether a Holder is Presenting a Lost, Stolen or Revoked Document at Border Crossing

States must work within existing national laws and respect international agreements relating to the use of travel documents and border control when processing travellers at their borders. All travellers with reported travel documents (lost, stolen, revoked) shall be treated as if no illegal intention existed, until otherwise proven.

6.4.1 When a travel document gets a "hit" on INTERPOL's lost, stolen or revoked database

A traveller should not be refused entry or prevented exit solely based on the document appearing on the lost, stolen or revoked travel document database. There are many steps that States must take to support these actions. If a traveller is in possession of a travel document that has been recorded as lost, stolen, or revoked on the ASF/SLTD, States should, where possible, liaise with the issuing and reporting country to confirm that the document has been rightfully recorded as a lost, stolen or revoked travel document. States should also conduct an interview with the traveller to ascertain his true identity or nationality, and determine if he is the rightful bearer of the travel document.

If the document contains a chip, States should conduct biometric verifications to support their efforts to determine the true identity of the traveller. States should also make efforts to determine whether the data have been altered and whether the document is authentic.

6.4.2 Processing the rightful owner of the travel document through border control

In dealing with the rightful owners of travel documents, States should be cognizant that those identified as the rightful bearers of a travel document declared lost, stolen or revoked are not necessarily attempting to commit a criminal offense. Rather than focusing on penalizing these individuals, States should focus on identifying ways of removing these documents from circulation, while minimizing disruption to travel. Where permitted under national law, States may consider alternate methods of dealing with these travellers from ways of dealing with those that are intentionally attempting to illegally enter the country by committing identity fraud.

Travellers entering a foreign country on a document declared lost, stolen or revoked as a result of a data error	Border control in the receiving State should contact the issuing authority to confirm the data error. Once confirmed, States may process the document as a valid travel document, but should advise the traveller to contact the issuing authority upon return to his country. Travel document issuing authorities in the issuing State should take all the necessary steps to have this document removed from the lost, stolen and revoked database. States should also consider replacing the affected document at no cost to the holder.
Nationals attempting to leave their country on a document declared lost or stolen	Where exit controls exist, border control should advise these travellers that their documents are not valid for travel, and that they must obtain a valid travel document before embarking on their journey, as lost, stolen and revoked travel documents are considered to be invalid.
Nationals attempting to leave their country on a revoked document	Where exit controls exist, border control should consult with national law enforcement to determine what measures/laws may be invoked to prevent the traveller from leaving the country. If permitted, border management/police authorities should prevent travellers from leaving the State.
Nationals attempting to leave a country and return to their country on a document declared lost, stolen or revoked	Where exit controls are in place and the identity and nationality of the holder have been confirmed, border control may allow the traveller to proceed, but should advise him that the document presented is not valid and that he may be refused boarding by the carrier. When a traveller is re-entering his country of origin on a document declared lost, stolen or revoked, border control may, where permitted by national law and/or international agreement, seize or impound the document to return it to the issuer. If their documents have been seized or impounded, travellers should be advised to obtain new valid travel documents.
Nationals attempting to leave a foreign country and continue to a third country on a document declared lost, stolen or revoked	Where exit controls are in place, border control should advise the travellers that their travel documents are invalid, that they may be refused boarding by the carrier, and that they may face difficulties upon arrival at their next destination.
Travellers entering a foreign country on a	Travellers who have been permitted to board should be advised

document declared lost, stolen or revoked	by the receiving State to contact their consulate or embassy to obtain a valid travel document before attempting to continue on their journey. Travellers that have not been permitted to enter may be dealt with according to national law.

6.4.3 Processing a traveller after determining that he is not the rightful owner of a document declared lost, stolen or revoked

Once it is determined that a traveller is not the rightful bearer of a document, border/police authorities from the sending or receiving State should seek to determine how the traveller came into possession of the document, including whether there was collusion with the rightful owner, and should domestic law permit, working in cooperation with the issuing State, determine whether additional fraudulent documents have been issued in that identity. If it is determined that the traveller has presented a lost, stolen or revoked travel document, States should investigate the traveller, and where applicable apply criminal charges and/or removal from their State.

States should confiscate documents for the purposes of legal proceedings, including immigration and refugee processing, but should return these to the issuing State once they have served this purpose. Efforts should also be made to provide the issuer with as much information about the interception as possible, should domestic law permit.

States should also ensure that inadmissible persons are documented in accordance with the provisions of ICAO Annex 9 — *Facilitation* to the Convention on International Civil Aviation.

7. REFERENCES (NORMATIVE)

Certain provisions of international Standards, referenced in this text, constitute provisions of Doc 9303. Where differences exist between the specifications contained in Doc 9303 and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, including machine readable visas, the specifications contained herein shall prevail.

Annex 9 Convention on International Civil Aviation (“Chicago Convention”), Annex 9 – *Facilitation.*

[ICAO EOI] ICAO TRIP Guide on Evidence of Identity, available at https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

— END —

APPENDIX A TO PART 2 — SECURITY STANDARDS FOR MRTDS (INFORMATIVE)

A.1 SCOPE

This Appendix provides advice on strengthening the security of machine readable travel documents made in accordance with the specifications set out in Doc 9303. The recommendations cover the security of the materials used in the document's construction, the security printing and copy protection techniques to be employed, and the processes used in the production of document blanks. Also addressed are the security considerations that apply to the personalization and the protection of the biographical data in the document. All travel document issuing authorities shall consider this Appendix.

A.2 INTRODUCTION

This Appendix identifies the security threats to which travel documents are frequently exposed and the counter-measures that may be employed to protect these documents and their associated personalization systems. The lists of security features and/or techniques offering protection against these threats have been subdivided into: 1) basic security features and/or techniques considered essential and; 2) additional features and/or techniques from which States are encouraged to select items which are recommended for providing an enhanced level of security.

This approach recognizes that a feature or technique that may be necessary to protect one State's documents may be superfluous or of minor importance to another State using different production systems. A targeted approach that allows States flexibility to choose from different document systems (paper-based documents, plastic cards, etc.) and a combination of security features and/or techniques most appropriate to their particular needs is therefore preferred to a "one size fits all" philosophy. However, to help ensure that a balanced set of security features and/or techniques is chosen, each State must conduct a risk assessment of its national travel documents to identify their most vulnerable aspects and select the additional features and/or techniques that best address these specific problems.

The aim of the recommendations in this Appendix is to improve the security of machine readable travel documents worldwide by establishing a baseline for issuing States. Nothing within these recommendations shall prevent or hinder States from implementing other, more advanced security features, at their discretion, to achieve a standard of security superior to the minimum recommended features and techniques set forth in this Appendix.

A summary table of typical security threats relating to travel documents and some of the security features and techniques that can help to protect against these threats is included.

A.3 BASIC PRINCIPLES

Production and storage of passport books and travel documents, including the personalization processes, should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. If the personalization process is decentralized, or if personalization is carried out in a location geographically separated from where the travel document blanks are made, appropriate precautions should be taken when transporting the blank documents and any associated security materials to safeguard their security in transit and storage on arrival. When in transit, blank books or other travel documents should contain the unique document number. In the case of passports the passport number should be on all pages other than the biographical data page where it can be

printed during personalization.

There should be full accountability over all the security materials used in the production of good and spoiled travel documents and a full reconciliation at each stage of the production process with records maintained to account for all security material usage. The audit trail should be to a sufficient level of detail to account for every unit of security material used in the production and should be independently audited by persons who are not directly involved in the production. Records certified at a level of supervision to ensure accountability should be kept of the destruction of all security waste material and spoiled documents.

Materials used in the production of travel documents should be of controlled varieties, where applicable, and obtained only from reputable security materials suppliers. Materials whose use is restricted to high security applications should be used, and materials that are available to the public on the open market should be avoided.

Sole dependence upon the use of publicly available graphics design software packages for originating the security backgrounds should be avoided. These software packages may however be used in conjunction with specialist security design software.

Security features and/or techniques should be included in travel documents to protect against unauthorized reproduction, alteration and other forms of tampering, including the removal and substitution of pages in the passport book, especially the biographical data page. In addition to those features included to protect blank documents from counterfeiting and forgery, special attention must be given to protect the biographical data from removal or alteration. A travel document should include adequate security features and/or techniques to make evident any attempt to tamper with it.

The combination of security features, materials and techniques should be well chosen to ensure full compatibility and protection for the lifetime of the document.

Although this Appendix deals mainly with security features that help to protect travel documents from counterfeiting and fraudulent alteration, there is another class of security features (Level 3 features) comprised of covert (secret) features designed to be authenticated either by forensic examination or by specialist verification equipment. It is evident that knowledge of the precise substance and structure of such features should be restricted to very few people on a “need to know” basis. Among others, one purpose of these features is to enable authentication of documents where unequivocal proof of authenticity is a requirement (e.g., in a court of law). All travel documents should contain at least one covert security feature as a basic feature.

Important general standards and recommended practices for passport document validity period, one-person-one-passport principle, deadlines for issuance of Machine Readable Passports and withdrawal from circulation of non-MRPs and other guidance is found in ICAO Annex 9 — *Facilitation*.

There is no other acceptable means of data storage for global interoperability other than a contactless IC, specified by ICAO as the capacity expansion technology for use with MRTDs.

A.4 MAIN THREATS TO THE SECURITY OF TRAVEL DOCUMENTS

The following threats to document security, listed in no particular order of importance, are identified ways in which the document, its issuance and use may be fraudulently attacked:

- counterfeiting a complete travel document;
- photo substitution;
- deletion/alteration of data in the visual or machine readable zone of the MRP data page;

- construction of a fraudulent document, or parts thereof, using materials from legitimate documents;
- removal and substitution of entire page(s) or visas;
- deletion of entries on visa pages and the observations page;
- theft of genuine document blanks;
- impostors (assumed identity; altered appearance); and
- tampering with the contactless IC (where present) either physically or electronically.

Detection of security features can be at any or all of the following three levels of inspection:

- Level 1 – Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features);
- Level 2 – Examination by trained inspectors with simple equipment; and
- Level 3 – Inspection by forensic specialists.

To maintain document security and integrity, periodic reviews and any resulting revisions of document design should be conducted. This will enable new document security measures to be incorporated and to certify the document's ability to resist compromise and document fraud attempts regarding:

- photo substitution;
- delamination or other effects of deconstruction;
- reverse engineering of the contactless IC as well as other components;
- modification of any data element;
- erasure or modification of other information;
- duplication, reproduction or facsimile creation;
- effectiveness of security features at all three levels: cursory examination, trained examiners with simple equipment and inspection by forensic specialists; and
- confidence and ease of second level authentication.

To provide protection against these threats and others, a travel document requires a range of security features and techniques combined in an optimum way within the document. Although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100 per cent effective in eliminating any one category of threat. The best protection is obtained from a balanced set of features and techniques providing multiple integrated layers of security in the document that combine to deter or defeat fraudulent attack.

A.5 SECURITY FEATURES AND TECHNIQUES

In the sections that follow, security features, techniques and other security measures are categorized according to the phases passed through during the production and personalization processes and the components of the travel document created thereby with regard to:

1) substrate materials;

2) security design and printing;

3) protection against copying, counterfeiting or fraudulent alteration; and

4) personalization techniques.

Issuing States are recommended to incorporate all of the basic features/measures and to select a number of additional features/measures from the list having first completed a full risk assessment of their travel documents. Unless otherwise indicated, the security features may be assumed to apply to all parts of a travel document including the cover and the binding of the booklet and to all the interior pages of a passport, comprising the biographical data page, end leaves and visa pages. Care must be taken to ensure that features do not interfere with the machine readability of the travel document.

A.5.1 Substrate Materials

A.5.1.1 Paper forming the pages of a travel document

Basic features:

- UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;

- watermark comprising two or more grey levels in the biographical data page and visa pages;

- appropriate chemical sensitizers in the paper, at least for the biographical data page (if compatible with the personalization technique); and

- paper with appropriate absorbency, roughness and weak surface tear.

Additional features:

- watermark in register with printed design;

- a different watermark on the data page to that used on the visa pages to prevent page substitution;

- a cylinder mould watermark;

- invisible fluorescent fibres;

- visible (fluorescent) fibres;

- security thread (embedded or window) containing additional security features such as micro print and fluorescence;

- a taggant designed for detection by special equipment; and
- a laser-perforated security feature.

A.5.1.2 Paper or other substrate in the form of a label used as the biographical data page of a travel document

Basic features:

- UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- appropriate chemical sensitizers in the paper (not normally possible in a plastic label substrate);
- invisible fluorescent fibres;
- visible (fluorescent) fibres; and
- a system of adhesives and/or other characteristics that prevents the label from being removed without causing clearly visible damage to the label and to any laminates or overlays used in conjunction with it.

Additional features:

- security thread (embedded or window) containing additional security features such as micro print and fluorescence;
- a watermark can be used in the paper of a data page in paper label form;
- a laser-perforated security feature; and
- die cut security pattern within the label to create tamper evidence.

A.5.1.3 Security aspects of paper forming the inside cover of a passport book

Paper used to form the inside cover of a passport book need not have a watermark. Although definitely not recommended, if an inside cover is used as a biographical data page (see A.5.5.1), alternative measures must be employed to achieve an equivalent level of security against all types of attack as provided by locating the data page on an inside page.

The paper forming the inside cover should contain appropriate chemical sensitizers when an inside cover is used as a biographical data page. The chemically sensitized paper should be compatible with the personalization technique and the adhesive used to adhere the end paper to the cover material of the passport.

A.5.1.4 Synthetic substrates

Where the substrate used for the biographical data page (or inserted label) of a passport book or MRTD card is formed entirely of plastic or a variation of plastic, it is not usually possible to incorporate many of the security components described in A.5.1.1 through A.5.1.3. In such cases additional security properties shall be included, including additional security printed features, enhanced personalization techniques and the use of optically variable features over and above the recommendations contained in A.5.2 to A.5.5.2. States should preferably ensure that the plastic substrate is manufactured under controlled conditions and contains distinctive properties, e.g. controlled fluorescence, to differentiate it from standard financial card substrates.

Basic features:

- construction of the data page should be resistant to physical splitting into layers;
- UV dull substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners;
- appropriate measures should be used to incorporate the data page securely and durably into the machine readable travel document; and
- optically variable feature.

Additional features:

- windowed or transparent feature;
- tactile feature; and
- laser-perforated feature.

A.5.2 Security Printing

A.5.2.1 Background and text printing

Basic features (see Terms and Definitions *in Doc 9303-1):*

- two-colour guilloche security background design pattern[1];
- rainbow printing;
- microprinted text; and

1. Where the guilloche pattern has been computer-generated, the image reproduced on the document must be such that no evidence of a pixel structure shall be detectable. Guilloches may be displayed as positive images, where the image lines appear printed with white spaces between them, or as negative images, where the image lines appear in white, with the spaces between them printed. A two-colour guilloche is a design that incorporates guilloche patterns created by superimposing two elements of the guilloche, reproduced in contrasting colours.

- security background of the biographical data page printed in a design that is different from that of the visa pages or other pages of the document.

Additional features:

- single or multi-colour intaglio printing comprising a “black-line white-line” design on one or more of the end leaves or visa pages;
- latent (intaglio) image;
- anti-scan pattern;
- duplex security pattern;
- relief (3D) design feature;
- front-to-back (see-through) register feature;
- deliberate error (e.g. spelling);
- every visa page printed with a different security background design;
- tactile feature; and
- unique font(s).

A.5.2.2 Inks

Basic features:

- UV fluorescent ink (visible or invisible) on the biographical data page and all visa pages; and
- reactive ink, where the substrate of the document pages or of a label is paper, at least for the biographical data page (if compatible with the personalization technique).

Additional features:

- ink with optically variable properties;
- metallic ink;
- penetrating numbering ink;
- metameric ink;
- infrared drop-out ink;
- infrared absorbent ink;
- phosphorescent ink;

- tagged ink; and
- invisible ink which fluoresces in different colours when exposed to different wave lengths.

A.5.2.3 Numbering

It is strongly recommended that the unique document number be used as the passport number.

Basic features:

- the passport number should appear on all sheets of the document and on the biographical data page of the document;
- the number in a document shall be either printed and/or perforated;
- the document number on a label shall be in a special style of figures or typeface and be printed with ink that fluoresces under ultraviolet light in addition to having a visible colour;
- the number on a data page of a passport made of synthetic substrate or on an MRTD card can be incorporated using the same technique as is used for applying the biographical data in the personalization process; and
- for MRTD cards, the number should appear on both sides.

Additional features:

- if perforated, it is preferable that laser perforation be used. Perforate numbering of the data page is optional but, if used, care should be taken not to interfere with the clarity of the portrait or VIZ and not obstruct the MRZ in any way. It is desirable to perforate the cover of the passport; and
- if printed, it should ideally be in a special style of figures or typeface and be printed with an ink that fluoresces under ultraviolet light in addition to having a visible colour.

A.5.2.4 Special security measures for use with non-laminated biographical data pages

The surface of the data page should be protected against soiling in normal use including regular machine reading of the MRZ, and against tampering.

If a page of a document is used for biographical data that is not protected by a laminate or an overlay as a protective coating (see A.5.3.2, A.5.4.3 and A.5.4.4), additional protection shall be provided by the use of intaglio printing incorporating a latent image and microprinting and preferably utilizing a colour-shifting ink (e.g. ink with optically variable properties).

A.5.2.5 Special security measures for use with cards and biographical data pages made of plastic

Where a travel document is constructed entirely of plastic, optically variable security features shall be employed which give a changing appearance with angle of viewing. Such devices may take the form of latent images, lenticular features, colour-shifting ink, or diffractive optically variable image features.

A.5.3 Protection Against Copying

A.5.3.1 Need for anti-copy protection

The current state of development of generally available digital reproduction techniques and the resulting potential for fraud mean that high-grade security features in the form of optically variable features or other equivalent devices will be required as safeguards against copying and scanning. Emphasis should be placed on the security of the biographical data page of a passport book, travel card or visa, based on an independent, complex optically variable feature technology or other equivalent devices complementing other security techniques. Particular emphasis should be given to easily identifiable, visual or tactile features which are examined at Level 1 inspection.

Appropriate integration of optically variable feature components or other equivalent devices into the layered structure of the biographical data page should also protect the data from fraudulent alteration. The optically variable components and all associated security materials used to create the layered structure must also be protected against counterfeiting.

A.5.3.2 Anti-copy protection methods

Subject to the minimum recommendations described in A.5.4.3 and A.5.4.4 on the need for lamination, optically variable features should be used on the biographical data page of a passport book, travel card or visa as a *basic feature*.

When a biographical data page of a passport book, travel card or visa is protected by a laminate film or overlay, an optically variable feature (preferably based on diffractive structure with tamper-evident properties) should be integrated into the page. Such a feature should not affect the legibility of the entered data.

When the biographical data page is an encapsulated paper label, or a page in a passport, the biographical data must be suitably protected by a protective laminate or measures providing equivalent security in order to deter alteration and/or removal.

When the machine readable biographical data page of a passport book is made entirely of synthetic substrate, an optically variable feature should be incorporated. The inclusion of a diffractive optically variable feature is recommended to achieve an enhanced level of protection against reproduction.

Devices such as a windowed or transparent feature, a laser-perforated feature, and others considered to offer equivalent protection may be used in place of an optically variable feature.

When the travel document has no overlay or laminate protection, an optically variable feature (preferably based on diffractive structure) with intaglio overprinting or other printing technique shall be used.

A.5.4 Personalization Technique

A.5.4.1 Document personalization

This is the process by which the portrait, signature and/or other biographical data relating to the holder of the document are applied to the travel document. These data record the personalized details of the holder and are at the greatest risk of counterfeit or fraudulent alteration. One of the most frequent types of document fraud involves the removal of the portrait image from a stolen or illegally obtained travel document and its replacement with the portrait of a different person. Documents with stick-in portrait photographs are particularly susceptible to photo substitution. Therefore, stick-in photographs are NOT permitted in MRTDs.

A.5.4.2 Protection against alteration

To ensure that data are properly secured against attempts at forgery or fraudulent alteration it is very strongly recommended to integrate the biographical data, including the portrait, signature (if it is included on the biographical data page) and main issue data, into the basic material of the document. A variety of technologies are available for personalizing the document in this way, including the following, but not precluding the development of new technologies, which are listed in no particular order of importance:

- laser toner printing;
- thermal transfer printing;
- ink-jet printing;
- photographic processes; and
- laser engraving.

The same personalizing technologies may also be used to apply data to the observations page of the passport. Laser toner should not be used to personalize visas or other security documents that are not protected by a secure laminate.

Authorities should carry out testing of their personalization processes and techniques against malfeasance.

A.5.4.3 Choice of document system

The choice of a particular technology is a matter for individual issuing States and will depend upon a number of factors, such as the volume of travel documents to be produced, the construction of the document and whether it is to be personalized during the document or passport book making process or after the document or book has been assembled and whether a country issues passports centrally or from decentralized sites.

Whichever method is chosen, it is essential that precautions be taken to protect the personalized details against tampering. This is important because, even though eliminating the stick-in portrait reduces the risk of photo substitution, the unprotected biographical data remains vulnerable to alteration and needs to be protected by the application of a heat-sealed (or equivalent) laminate with frangible properties, or equivalent technology that provides evidence of tampering.

A.5.4.4 Protection against photo substitution and alteration of data on the biographical data page of a passport book

Basic features:

- personalizing the portrait and all biographical data by integration into the basic material;
- the security printed background (e.g. guilloche) shall merge within the portrait area;
- use of reactive ink and chemical sensitizers in the paper;
- a visible security device should overlap the portrait without obstructing the visibility of the portrait; an optically variable feature is recommended; and
- use of a heat-sealed (or equivalent) secure laminate, or the combination of an personalizing technology

and substrate material that provide an equivalent resistance to substitution and/or counterfeit of the portrait and other biographical data.

Additional features:

- displayed signature of the holder may be scanned and incorporated into the printing;
- steganographic image incorporated in the document;
- additional portrait image(s) of holder;
- machine-verifiable features as detailed in Doc 9303, Parts 9 through 12.

A.5.5 Additional Security Measures for Passport Books

A.5.5.1 Position of the biographical data page

It is recommended that States place the data page on an inside page (the second or penultimate page). When the data page is situated on the inside cover of an MRP, the normal method of construction used in the manufacture of passport covers has facilitated fraudulent attacks on the data page, typically photo substitution or whole-page substitution. However, an issuing State may place the data page on a cover provided that it ensures that the construction of the cover used in its passport offers a similar level of security against all types of fraudulent attack to that offered by locating the data page on an inside page. Placing the biographical data page on the cover is, nevertheless, strongly NOT recommended.

A.5.5.2 Whole-page substitution

Issuing States' attention is drawn to the fact that with integrated biographical data pages replacing stick-in photographs in passports, some cases of whole-page substitution have been noted in which the entire biographical data page of the passport has been removed and substituted with a fraudulent one. Although whole-page substitution is generally more difficult to effect than photo substitution of a stick-in photo, it is nevertheless important that the following recommendations be adopted to help in combating this category of risk. As with all other categories of document fraud, it is better to employ a combination of security features to protect against whole-page substitution rather than rely on a single feature which, if compromised, could undermine the security of the whole travel document.

Basic features:

- the sewing technology that binds the pages into the book must be such that it must be difficult to remove a page without leaving clear evidence that it has happened;
- security background of the biographical data page printed in a design that is different from that of the visa pages;
- page numbers integrated into the security design of the visa pages; and
- serial number on every sheet, preferably perforated.

Additional features:

- multi-colour and/or specifically UV fluorescent sewing thread;
- programmable thread-sewing pattern;
- UV cured glue applied to the stitching;
- index or collation marks printed on the edge of every visa page;
- laser-perforated security features to the biographical data page; and
- biographical data printed on an inside page in addition to the data page.

Where self-adhesive labels are used, additional security requirements as described in A.5.1.2 and A.5.2.4 are advised including linking the label to the machine readable travel document by the travel document number.

A.5.6 Quality Control

Quality checks and controls at all stages of the production process and from one batch to the next are essential to maintain consistency in the finished travel document. This should include quality assurance (QA) checks on all materials used in the manufacture of the documents and the readability of the machine readable lines. The importance of consistency in the finished travel document is paramount because immigration inspectors and border control officers rely upon being able to recognize fake documents from variations in their appearance or characteristics. If there are variations in the quality, appearance or characteristics of a State's genuine travel documents, detection of counterfeit or forged documents is made more difficult.

A.5.7 Security Control of Production and Product

A major threat to the security of the MRP of an issuing State can come from the unauthorized removal from the production facility of genuine finished, but unpersonalized, MRPs or the components from which MRPs can be made.

A.5.7.1 Protection against theft and abuse of genuine document blanks or document components

Blank documents should be stored in locked and appropriately supervised premises. The following measures should be adopted:

Basic measures:

- good physical security of the premises with controlled access to delivery/shipment and production areas, and document storage facilities;
- full audit trail, with counting and reconciliation of all materials (used, unused, defective or spoiled) and certified records of same;
- all document blanks and other security-sensitive components serially numbered with full audit trail for every document from manufacture to dispatch, as applicable;

- where applicable, tracking and control numbers of other principal document components (e.g. rolls or sheets of laminates, optically variable feature devices);
- secure transport vehicles for movement of blank documents and other principal document components (if applicable);
- details of all lost and stolen travel document blanks to be rapidly circulated between governments and to border control authorities with details sent to the INTERPOL lost and stolen database;
- appropriate controls to be in place to protect the production procedures from internal fraud; and
- security vetting of staff.

Additional measures:

- CCTV coverage/recording of all production areas, where permitted; and
- centralized storage and personalization of blank documents in as few locations as possible.

Table 1. Summary of security recommendations

Elements	*Basic features*	*Additional features*
Substrate materials (A.5.1)		
Paper substrates (A.5.1.1)	– controlled UV response – two-tone watermark – chemical sensitizers – appropriate absorbency and surface characteristics	– registered watermark – different watermark on the data page and visa page – cylinder mould watermark – invisible fluorescent fibres – visible (fluorescent) fibres – security thread – taggant – laser-perforated security feature
Paper or other substrate in the form of a label (A.5.1.2)	– controlled UV response – chemical sensitizers – invisible florescent fibres – visible (florescent) fibres – system of adhesives	– security thread – watermark – laser-perforated security feature – die cut security pattern
Synthetic substrates (A.5.1.4)	– construction resistant to splitting – optically dull material – secure incorporation of data page – optically variable features – see A.5.2 – A.5.5, as appropriate	– window or transparent feature – tactile feature – laser-perforated feature

Elements	*Basic features*	*Additional features*
Security printing (A.5.2)		
Background and text printing (A.5.2.1)	– two-colour guilloche background – rainbow printing – microprinted text – unique data page design	– intaglio printing – latent image – anti-scan pattern – duplex security pattern – relief design feature – front-to-back register feature – deliberate error – unique design on every page – tactile feature – unique font(s)
Inks (A.5.2.2)	– UV florescent ink – reactive ink	– ink with optically variable properties – metallic ink – penetrating numbering ink – metameric ink – infrared drop-out ink – infrared absorbent ink – phosphorescent ink – tagged ink – invisible ink
Numbering (A.5.2.3)	– numbering on all sheets – printed and/or perforated number – special typeface numbering for labels – identical technique for applying numbering and biographical data on synthetic substrates and cards	– laser-perforated document number – special typeface
Personalization technique (A.5.4)		
Protection against photo substitution and alteration (A.5.4.4)	– integrated biographical data – security background merged within portrait area – reactive inks and chemical sensitizers in paper – visible security device overlapping portrait area – heat-sealed secure laminate or equivalent	– displayed signature – steganographic image – additional portrait image(s) – biometric feature as per Part 9

Elements	*Basic features*	*Additional features*
Additional security measures for passport books (A.5.5)		
Page substitution (A.5.5.2)	– secure sewing technology – UV fluorescent sewing thread – unique data page design – page numbers integrated into security design – serial number on every sheet	– multi-colour sewing thread – programmable sewing pattern – UV cured glue to stitching – index marks on every page – laser-perforated security feature – biographical data on inside page
Security control of production and product (A.5.7)		
Protection against theft and abuse (A.5.7.1)	– good physical security – full audit trail – serial numbers on blank documents, as applicable – tracking and control numbers of components, as applicable – secure transport of blank documents – international information exchange on lost and stolen documents – internal fraud protection procedures – security vetting of staff	– CCTV in production areas – centralized storage and personalization

Note 1.— The list of additional features is not exhaustive, and issuing States and organizations are encouraged to adopt other security features not explicitly mentioned in this Appendix.

Note 2.— The descriptions in the table above are necessarily abbreviated from the main text. For ease of reference, the relevant sections of this Appendix are referenced by the paragraph numbers in parentheses in the "Elements" column of the above table.

Note 3.— Certain of the features are repeated one or more times in the table. This indicates that the particular feature protects against more than one type of threat. It is only necessary to include these features once within any particular document.

Note 4.— There are many other factors associated with passport security than are elaborated here. Appendices B and C provide additional guidance. Therefore, Appendices A, B and C need to be considered collectively to ensure document issuance integrity.

Note 5.— Any reference, direct or implied, to specific terms and/or technologies are solely intended to capture the terms and technologies in their generic form and do not have any association with specific vendors or technology providers.

— — — — — — — —

APPENDIX B TO PART 2 — MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION (INFORMATIVE)

B.1 SCOPE

This Appendix contains recommendations which cover machine authentication of the security features in the document itself (based on materials, on security printing and on copy protection techniques) as well as advice on reader technologies that allow for machine authentication of documents.

B.2 DOCUMENT READERS AND SYSTEMS FOR MACHINE AUTHENTICATION

In order to verify traditional as well as innovative security features of MRTDs, it is important to have reading technology in place which accommodates the wide variety of travel documents in circulation. These readers have to be equipped with the appropriate sensors for the more common and advanced machine authentication features. This, of course, is a worldwide cost and infrastructure issue.

B.2.1 Standard Readers

Standard readers which are deployed at borders usually have the following hardware sensors:

- VIS, UV, IR illumination and high resolution image grabbing capabilities (minimum resolution 300 dpi) – this allows for reading the MRZ (preferably in the IR spectral range) and image processing of other features (in the VIS spectral range); and
- ISO 14443 compliant contactless IC readers (@ 13.56 MHz frequency).

Generally, standard readers are able to detect and verify the following security features:

- MRZ read and check digit verification;
- Contactless IC read and Passive Authentication (and, optionally, Active Authentication); and
- generic security checks (UV dull paper, IR readable MRZ, …).

Further “intelligence” of these readers solely depends on software, not on extra hardware sensors, and would therefore easily be deployed at the discretion of the receiving State without investing extra money for dedicated equipment. Software capabilities of readers may include:

- pattern recognition using databases (based on VIS, UV and IR images);
- read and authenticate digital watermarks (steganographic features) to check for authentic issuance;

- detect and read out (alphanumeric) displays and their future security features; and
- detect and read out LED-in-plastic based security features.

B.2.2 Advanced Readers

Additionally, advanced readers may have the following hardware sensors, suited to authenticate special security features:

- coaxial illumination for the verification of retro-reflective security overlays;
- laser diode or LED illumination for the verification of special structure features, e.g. for optically diffractive devices (DOVIDs);
- magnetic sensors for special substrate features, e.g. for the verification of magnetic fibres;
- spectral analysis or polarization detection devices; and
- transmission illumination of the MRP data page for the verification of registered watermarks, laser perforation, window-features and see-through registers – needs a special reader geometry to allow for the placement of the data page only (no cover behind) on the reader.

Usually, advanced reading capabilities are all based on national/bilateral/multilateral/proprietary agreements and require dedicated hardware.

B.2.3 Background Systems, Public Key Infrastructure (PKI)

To authenticate certain types of machine verifiable features, a background system or a PKI may be necessary. This could be the existing MRTD PKI (the ICAO PKD being the most prominent part) where States may exchange information on their security features within the logical data structure, secured by means of certificates.

B.3 SECURITY FEATURES AND THEIR APPLICATION FOR MACHINE AUTHENTICATION

The following paragraphs describe major security features and techniques as identified in Appendix A on Security Standards and explain how machine authentication could be deployed for these security mechanisms. Issuing Authorities which select security features from Appendix A may use the tables below to check which possibilities of machine authentication exist for such features.

B.3.1 Substrate Materials

B.3.1.1 Paper forming the pages of a travel document

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Controlled UV response		X					UV intensity
Two-tone watermark					Transmission	F	pattern matching
Chemical sensitizers							N/A
Appropriate absorbency and surface characteristics							N/A
Additional features							
Registered watermark					Transmission	F	pattern matching
Different watermark on the data page and visa page					Transmission	F	pattern matching*
Cylinder mould watermark					Transmission	F	pattern matching
Invisible fluorescent fibres		X	X			F/V	pattern matching
Visible (fluorescent) fibres	X	X				F/V	pattern matching
Security thread	X	X			Transmission, Magnetic	F	pattern matching
Taggant					Special	F/V	Depends on taggant
Laser-perforated security feature					Transmission	F/V	pattern matching

* User interaction required and not suitable for Automated Border Control systems

B.3.1.2 Paper or other substrate in the form of a label

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Controlled UV response		X					UV intensity
Chemical sensitizers							N/A
Invisible fluorescent fibres		X	X			F/V	pattern matching
Visible (fluorescent) fibres	X	X				F/V	pattern matching
System of adhesives							N/A
Additional features							
Security thread	X				Transmission, Magnetic	F	pattern matching
Watermark					Transmission	F	N/A
Laser-perforated security feature					Transmission	F/V	pattern matching
Die cut security pattern					Transmission	F	pattern matching

B.3.1.3 Synthetic substrates

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Construction resistant to splitting							N/A
Optically dull material		X					UV intensity
Secure incorporation of data page							N/A
Optically variable features							See A.5.3

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
See A.5.2 – A.5.5, as appropriate							
Additional features							
Window or transparent feature					Transmission	F	pattern matching
Tactile feature					Retro-reflective	F/V	pattern matching
Laser-perforated feature					Transmission	F/V	pattern matching
Surface characteristics	X		X		Retro-reflective	F	pattern matching

B.3.2 Security Printing

B.3.2.1 Background and text printing

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Two-colour guilloche background	X	X	X			F	Pattern matching
Rainbow printing	X	X			High res camera	F	Pattern matching
Microprinted text	X	X	X		High res camera	F	Pattern matching
Unique data page design	X					F	Pattern matching
Additional features							
Intaglio printing	X	X	X			F	Pattern matching*
Latent image							N/A
Anti-scan pattern	X				High res camera	F	Pattern matching
Duplex security pattern					Transmission	F	Pattern matching*
Relief design feature					Retro-reflective	F	pattern matching

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Front-to-back register feature					Transmission	F	Pattern matching
Deliberate error	X	X	X			F	OCR, Pattern matching
Unique design on every page	X	X				F	Pattern matching[#]
Tactile feature					Retro-reflective	F	pattern matching
Unique font(s)	X	X	X				Pattern matching

* Impractical implementation for passport readers

[#] User interaction required and not suitable for Automated Border Control systems

B.3.2.2 Inks

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
UV florescent ink		X				F/V	Pattern matching
Reactive inks					Special		Depending on ink
Additional features							
Ink with optically variable properties	X				Variable illumination	F/V	Pattern matching
Metallic ink			X			F/V	Pattern matching
Penetrating numbering ink					Special	V	Pattern matching on both sides
Metameric inks	X	X	X			F	Optical filters and Pattern matching
Infrared dropout ink	X		X			F/V	Pattern matching
Infrared absorbent ink			X			F/V	Pattern matching
Phosphorescent ink		X	X			F/V	Pattern matching

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Tagged ink					Special	F	Pattern matching
Invisible ink		X	X			F	Pattern matching
Magnetic ink					Magnetic	F/V	Pattern matching
Anti-Stokes-Ink			X			F/V	Optical filters and pattern matching

B.3.2.3 Numbering

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Numbering on all sheets Printed and/or perforated number	X		X			F/V	OCR, Pattern matching
Special typeface numbering for labels	X		X			F/V	OCR, Pattern matching
Identical technique for applying numbering and biographical data on synthetic substrates and cards							N/A
Additional features							
Laser-perforated document number					Transmission	F/V	Pattern matching
Special typefonts	X					F/V	OCR, Pattern matching

B.3.3 Protection Against Copying

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Optically variable features on the biographical data page	X				Variable illumination	F/V	Pattern matching
OVD with intaglio overprint if no laminate							N/A
Additional features							
Machine readable diffractive optically variable feature					Laser	F/V	decoding
Laser-perforated security feature					Transmission	F/V	Pattern matching
Anti-scan pattern	X				High res camera	F	Pattern matching

B.3.4 Personalization Techniques

B 3.4.1 Protection against photo substitution and alteration

Security Features	Sensor needed for Machine Authentication					Pattern fix/variable	Machine Authentication method
	Standard reader				Advanced reader		
	VIS	UV	IR	RF	Special sensor		
Basic features							
Integrated biographical data							N/A
Security background merged within portrait area							N/A
Reactive inks and chemical sensitizers in paper							N/A
Visible security device overlapping portrait area	X				Variable illumination	F/V	Pattern matching
Heat-sealed secure laminate or equivalent	X					F/V	Pattern matching

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Additional features							
Displayed signature							N/A
Steganographic feature	X	X	X			F/V	Decoding
Additional portrait image(s)	X	X	X	X		V	Pattern matching
Biometric feature as per Part 9				X		V	RF reader

B 3.5 Additional Security Measures for Passport Books

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
Secure sewing technology							N/A
UV fluorescent sewing thread		X				F	Pattern matching
Unique data page design	X					F	Pattern matching
Page numbers integrated into security design	X	X			High res camera		Pattern matching
Serial number on every sheet							N/A
Additional features							
Multi-colour sewing thread	X	X				F	Pattern matching
Programmable sewing pattern	X	X				F	Pattern matching
UV cured glue to stitching							N/A
Index marks on every page							N/A
Laser-perforated security feature					Transmission	F/V	Pattern matching
Biographical data on inside page							N/A

B 3.6 Additional Security Measures Suited for Machine Authentication

The following security features are suited for machine authentication but are not listed in Appendix A.

Security Features	*Sensor needed for Machine Authentication*					*Pattern fix/variable*	*Machine Authentication method*
	Standard reader				*Advanced reader*		
	VIS	*UV*	*IR*	*RF*	*Special sensor*		
Basic features							
MRZ read and check digit verification	X		X			F/V	Checksum calculation
Contactless IC read and Passive Authentication (+AA)				X			RF reader
Detect and read out LED-in-plastic based security features	X	X	X	X		F/V	Use R/F to power LED in plastic
Detect and read out (alphanumeric) displays and their future security features	X	X	X	X		F/V	Use R/F to power display in plastic
Detect and verify retro-reflective foil material	X				Coaxial lighting	F/V	Pattern matching
Barcodes	X	X	X			V	Decoding

B.4 SELECTION CRITERIA FOR MACHINE VERIFIABLE SECURITY FEATURES

If an issuing State considers incorporating security features for machine authentication in its MRTDs or a receiving State plans to deploy reader systems that are able to machine authenticate MRTDs, various criteria for the selection of these features have to be considered.

Much like the selection process for the global interoperable biometric or the storage technology, these criteria comprise:

- security – the most important criterion;
- availability, but exclusiveness for security documents (preferably more than one supplier available);
- dual-use, i.e. additional purpose of the feature beyond machine authentication, e.g. general anti-copy property or visual inspection;
- potential of the Machine Authentication feature to be personalized (i.e. individualized) with information from the passport to secure the personal data (e.g. the passport number, name) in order to avoid re-use of parts of genuine passports;
- compatibility to issuing processes for MRTDs;

- compatibility (to existing and standardized properties of MRTDs);
- compatibility to control process at the border and elsewhere (e.g. no obstruction of basic security features, no extra time needed);
- interoperability;
- sensor availability;
- cost (for feature and sensor);
- Intellectual Property (IP) issues, e.g., patents;
- primary inspection vs. secondary;
- time required to actually utilize the feature;
- potential difficulties associated with the book manufacturing and/or the personalization processes; and
- durability, i.e. according to the relevant ISO and ICAO specifications for MRTDs.

— — — — — — — —

APPENDIX C TO PART 2 — OPTICAL MACHINE AUTHENTICATION (INFORMATIVE)

C.1 INTRODUCTION

For the authentication of machine readable travel documents (MRTDs) as part of stationary border control as well as ABC gates, the use of IT systems, which go beyond the pure extraction and checking of the documents' MRZ and also automatically inspect optical security features, increases. The major improvements in technologies used in the context of machine based document authentication have contributed to the growth of the amount and diversity of the authentication systems. However, the significant increasing traveler volume still remains challenging for all actors involved in the design, production and deployment of authentication systems and MRTDs.

Authentication systems used to perform machine authentication of MRTDs include several components that are required to properly interact with each other. Furthermore, the security features of machine-readable documents need to be designed and implemented in accordance with the capabilities of the authentication systems and the insight of experienced practitioners.

This Appendix provides a set of recommendations for the main parties involved in the design, implementation and operation of the affected systems and key components, whereby the main goals are:

- increase the awareness for the relevant security-related questions of machine authentication, involving the main stakeholders e.g. security document producers, reading equipment manufacturers and government,
- propose a catalogue of generic check routines with a consistent terminology,
- define recommendations for security document designers, manufacturers of authentication systems, and operational level.

This Appendix is meant to support practitioners in the design, development of authentication systems. It is however important to bear in mind that the authentication system should be used to facilitate adjudication for its operator[1], and should not be regarded as decision maker by itself, particularly with regards to the security features that cannot be checked by the machine and can only be verified by a human operator.

This Appendix only deals with the optical part of the authentication of MRTDs and the scope of the recommendations is limited to data acquired through Full Page Readers, i.e. full size images of the document, as described in Appendix B of this Part. Furthermore, the Guidelines do not distinguish between 1st, 2nd and 3rd level inspection as full page readers can be used in each of those scenarios. Altogether, mobile devices are (so far) not taken into consideration due to their limited optical capabilities with respect to different light sources (neither UV nor IR) and therefore not being able to meet the proposed requirements.

[1] Operator: A person who directly interacts with the authentication system (e.g. manual interaction with the document reader) in the context of a document check.

The basics and terminology required for a better understanding of Optical Machine Authentication are introduced in section C.2. The issue of harmonization and standardization of check routines is addressed in section C.3, where a catalogue of generic check routines will be defined. In section C.4 the focus will be put on elaborated recommendations for manufacturers of authentication systems, and section C.5 will highlight several approaches and methodologies related to data procession in accordance with data protection policies.

C. 1.1 Terminology

Although the recommendations and guidelines are non-binding for the parties directly affected by it, the terminology has been adopted and integrated into Part 1 of Doc 9303 in order to provide an unambiguous description of what should be observed in order to achieve the goals defined in this document.

The terminology should be regarded as a practical way to organize the recommendations and guidelines in order of importance, and should not be mistaken with a set of restrictive requirements similar to those used in classical standards (e.g. ISO). In order to provide the target group with clear, precise and unambiguous guidance as to what is and is not in line with best practices, the present terminology is being used.

C. 1.2 Influence of the electronic check on the authentication process

Although focus is on the optical part of the authentication of MRTDs, the electronic part has to be taken into consideration. Based on current state of technology, the interaction between a chip (eMRTD) and an RF module (full page reader) during the authentication process is highly probable and can be expected. Some of the recommendations given in this document are best understood when keeping in mind that both optical and electronic checks (if applicable) are complementary processes converging to an overall result.

Two aspects of the interaction between electronic and optical checks are of particular interest: the comparison of optical and electronic data and the implications behind the check for presence of a chip if one is expected. For these two aspects, the influence of the electronic check cannot be disregarded and will be highlighted in the corresponding recommendations.

C.2 DEFINITIONS

In the following chapter, a consistent terminology will be introduced for further use. The process of inspection of MRTDs is described in general in section **Error! Reference source not found.**, and in detail in section **Error! Reference source not found.**. In section **Error! Reference source not found.** the influence of the electronic part of the authentication process is being addressed.

C. 2.1 Process of Identification and Verification of MRTDs

The authenticity verification of a travel document includes the verification of the document's optical security features. It is performed by an authentication system[2] which consists of the following components: a full page reader, authentication software[3], an authentication database and optionally a reference database.

The full page reader creates full size images of the travel document to be verified under different light sources. This so-called *live data-set* (=full size images of the document)[4] is transferred to the authentication software by the full page reader.

The authentication software usually identifies the so-called *document model* of the document using the Machine Readable Zone (MRZ) and/or additional information (e.g. document specific pattern, date of issue, specific optical features, etc.) as input. A document model covers those document series of a nation which have the same optical appearance.

In accordance to the technical guideline [BSI-TR-03135], a document model is defined by means of the country code (C), document type (T), a unique identification number (N) and the year value of first issuance (Y):

Document Model := (C, T, N, Y) [5]

The country code C has to be filled in according to the ICAO Doc 9303 specifications as a three-letter code.

The document type T is also specified by ICAO in Doc9303.

The identification number N must be a unique chronological increasing integer number starting with 1 referencing the model – or generation – of the document.

The year Y refers to the year as a 4-digit integer value in which a document of that particular model was issued for the first time. If the year is unknown, this value shall be omitted.

For instance, the two British passport/document models from 2008 and 2010 in circulation have the following identifiers: (GBR, P, 1, 2008) and (GBR, P, 2, 2010).

There are various technical approaches for identifying the document model. MRZ acquisition is one of them (cf. section C.4.3.2). If the MRZ is used but not sufficient for the unambiguous determination of the document model, additional document parameters (e.g. patterns) have to be used to help narrow down the identification results; especially when dealing with several valid document models of the same country (e.g. British passport)[6].

---

[2] An authentication system describes the combination of a full page reader, authentication software incl. authentication database and optionally the expert reference database.

3 The authentication software receives the live data-set from the full page reader. It provides several authentication algorithms in order to apply the check routines to the live data-set.

4 Live data-set: The visual-, IR-, and UV-picture of the document under test to be verified with the reader system. These pictures are used for the document's inspection.

[5] This Appendix only focus on the optical part of machine-based document authentication. This means that documents that are optically identical but differ when considering electronic features, are considered to belong to the same document model.

[6] Some countries, such as Australia, use a series' Letter to distinguish different document models or series (e.g. N-series). Even though this method might be sufficient at national level, it is not very efficient for international classification because of the lack of standardisation. Therefore, this document follows the recommendations of [BSI-TR-03135] which are considered to be more suitable for that purpose.

The authentication software sends the document model's identifier to the authentication database where the so-called *check routines* are stored. These check routines define which testing procedures have to be applied to the live data-set of this particular travel document model. A specific set of check routines, the so-called *authentication data-set*, is determined for each document model. After the receipt of the document model's identifier, the authentication database sends the corresponding data-set to the authentication software. Further details on the setup of an authentication database will be provided in section C.2.2.

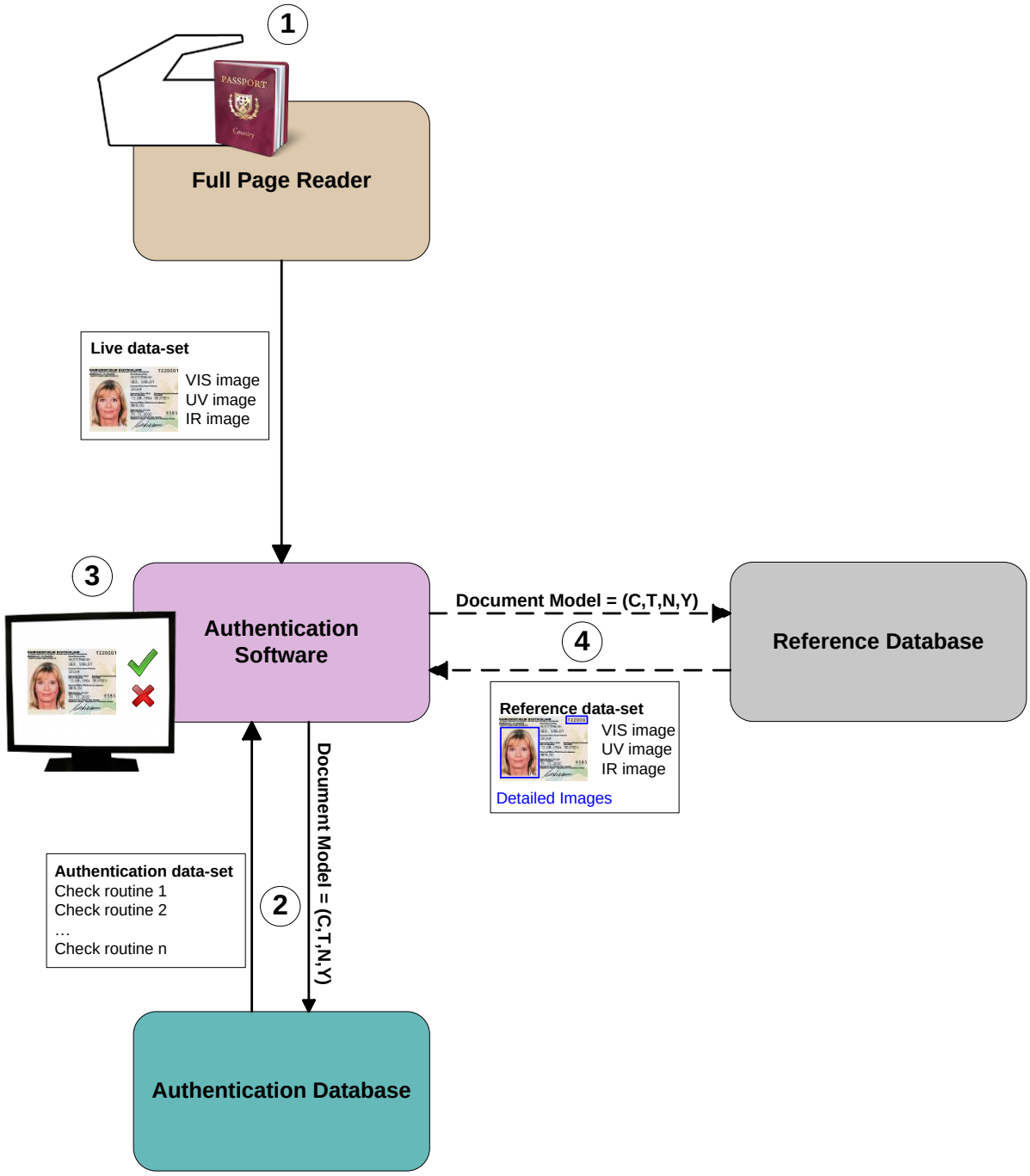


Figure 0–1: Process of document identification and verification; the numbers denote the order of the involved process steps

The verification is now performed by the authentication software. The check routines are applied to the travel document's live data-set. This examination usually leads to a Pass- or Fail-result. A Pass-result implies that the checked document

does not present any abnormalities, whereby a Fail-result means the opposite. Depending on the application scenario, the interpretation of the result (pass or fail) is the responsibility of the human operator.

If a live data-set cannot be assigned unambiguously to a particular document model, a subset of check routines should be performed optionally. These check routines are specified independently of the document model.

In order to support the human operator in a manual verification, the authentication software can request the so-called *reference data-set* from the reference database on the basis of the identified document model. The reference data-set contains the visible-light (white), IR and UV images of the document model and can also include more detailed pictures of document parts as well as further textual descriptions. However, this so-called reference database, also referred to as *expert database* in practice, is not a mandatory component of the actual authentication system. The process of document identification and verification is illustrated in Figure 0–1.

C. 2.2 Detailed Setup of an Authentication Database

In the authentication database a distinct set of check routines is stored for each document model. For instance, the check routines for the German document model from 2007 differ from the routines which have to be applied to the British document model from 2008.

A check routine of a set denotes a test specification for an optical security feature's property. E.g. the check routine 1 in Figure 0–2 checks whether the photo is absorbent in visible light. In this case the photo is the optical feature, which is tested for the property of absorption under visible light (see light source  in check routine 1). The implementation of this check routine is carried out by an authentication algorithm provided by the authentication software (see authentication algorithm  in check routine 1). In this case, algorithm 1 is an authentication algorithm which checks the feature's brightness. In contrast, check routine x in Figure 0–2 checks whether or not the ink is luminescent under UV light within the area of the photo by using the "pattern check" algorithm (check algorithm n of the authentication software on Figure 0–2). This example shows clearly that an optical security feature can offer different properties under different light sources (see Figure 0–3).

In terms of the EU regulation on minimum standards for security features and biometrics in passports and travel documents these check routines can be reasonably split into the three categories: material, printing technique and personalization.

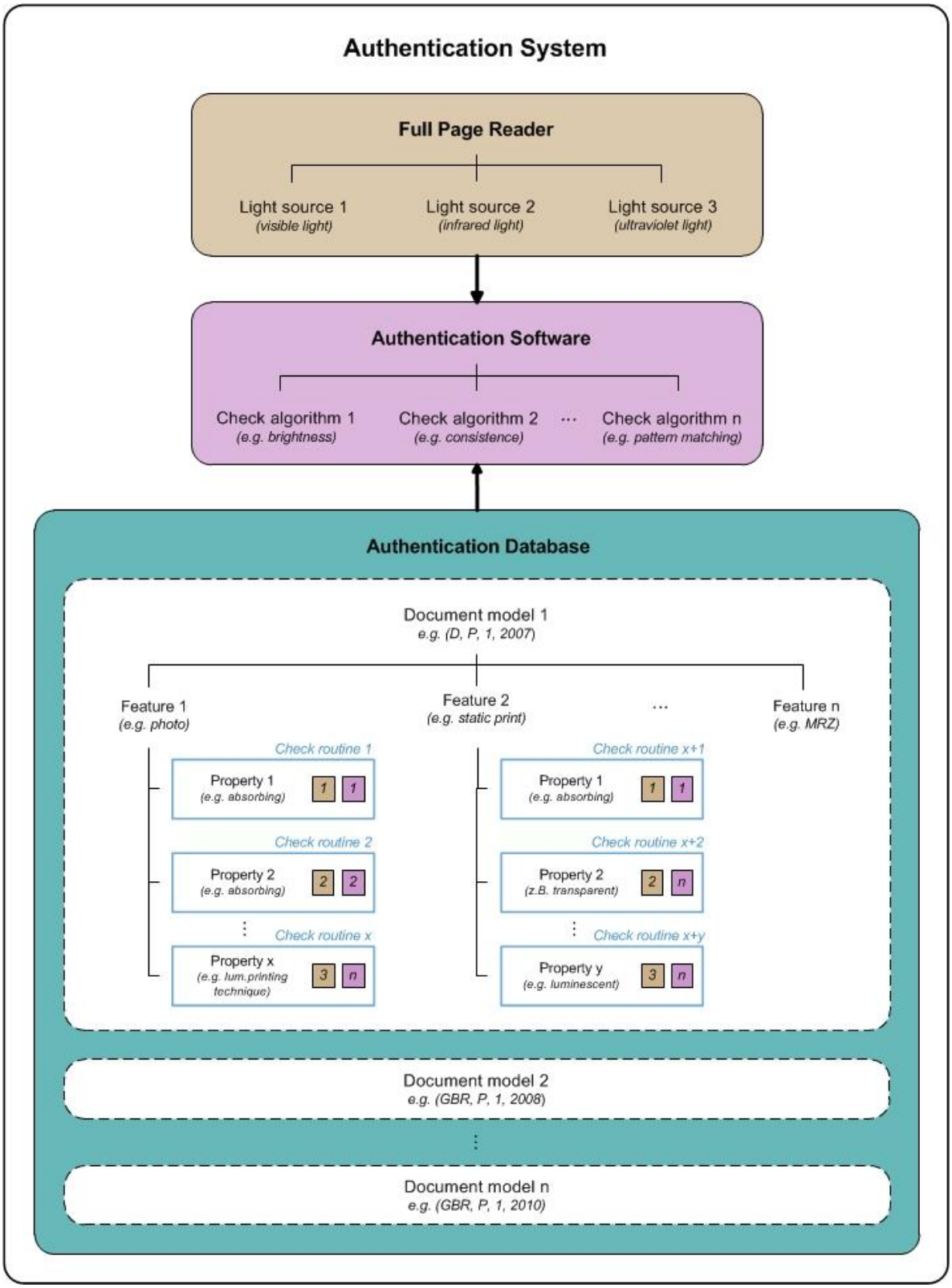


Figure 0–2: Schematic diagram of the setup of an authentication system

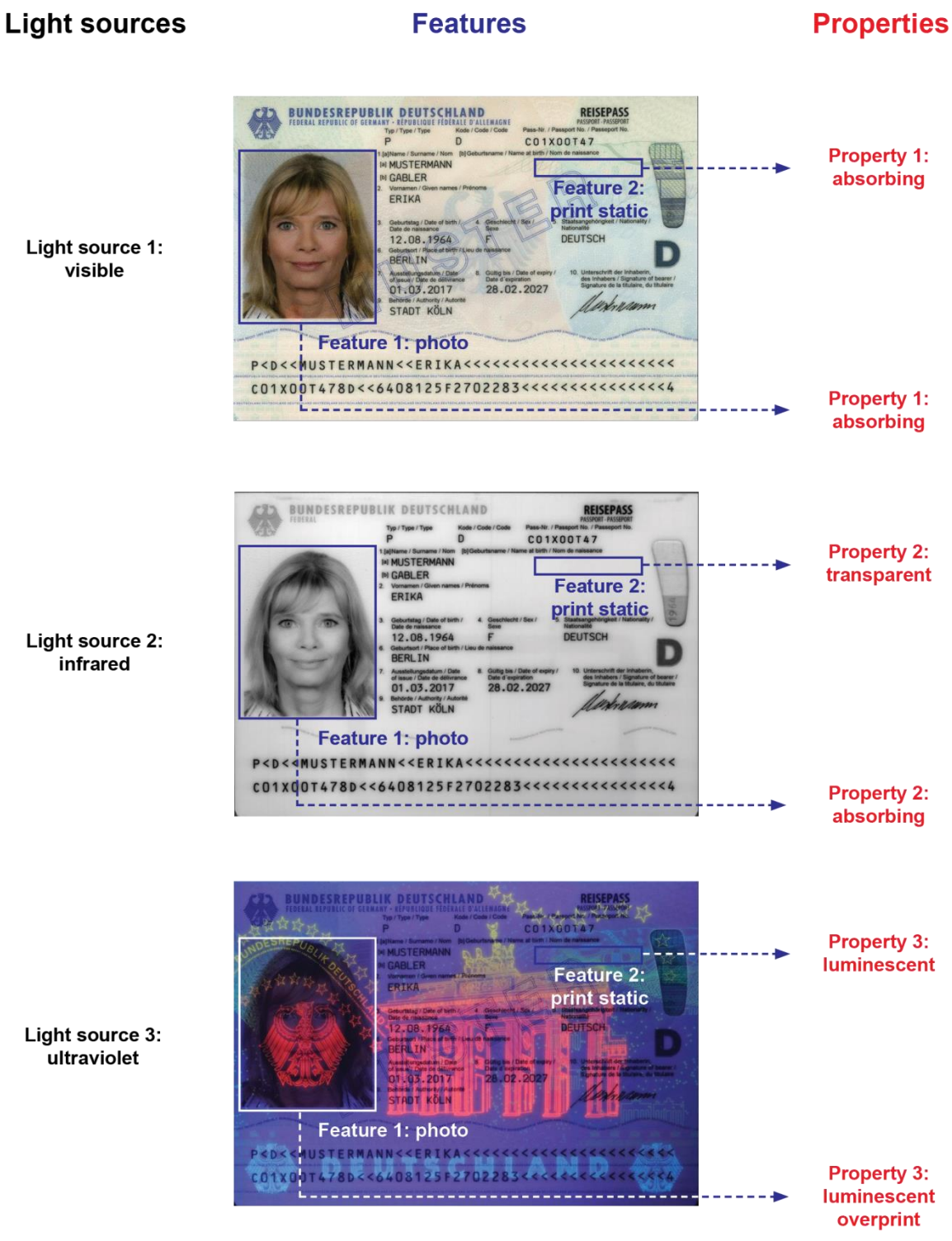


Figure 0–3: Features and properties under different light sources using the example of the German passport

C.3 CATALOGUE OF GENERIC CHECK ROUTINES

Every developer of an authentication system defines his own identifiers for the check routines. On the one hand these check routines are distinct for each document model. On the other hand the identifiers for these check routines are often not self-explanatory. Hence, the comparability of the applied check routines for the same document model for different authentication systems is in general not existent.

In order to solve this problem, it is possible to define a catalogue of feasible check routines on the basis of the spectrally selective security features in travel documents. The content of this catalogue may be extended in future versions of this guideline preserving the proposed nomenclature. The corresponding so-called *spectrally selective check routines* record different reactions occurring on a document checked under visible (VI - visible light) or extra visible (UV - ultraviolet, IR - infrared) light. Based on the three records (VI, UV, IR), the absorbent, reflective or luminescent reactions of these features can be checked. Sequentially these spectrally selective check routines will be denoted by *generic check routines* as defined in the [BSI-TR-03135].

The application of this catalogue of generic check routines would greatly improve the above mentioned situation and will allow for a better understanding of machine authentication mechanisms.

C. 3.1 Description of Generic Check Routines

The below defined unambiguous identifiers of check routines have been defined for the optical machine authentication on the basis of the spectral reaction of security features in travel documents. They can be reasonably split into the following four categories defined in in ICAO Doc9303 Part 2 Appendix A:

- Check for material (substrate) properties: Reactions of the printing substrate are verified, e.g. brightness under UV light
- Check for printing technique properties: Features, which are printed onto/into the document irrespective of personalization, are tested, e.g. form print
- Check for features that protect copying: usually diffractive or holographic elements or laminates
- Check for issuing technique (personalization) properties: Personalized features are tested, e.g. the name of the document's holder

The optical appearance of the features of the category "copy protection" is very dependent on illumination geometry. Therefore features of this category– well suited for human inspection – can be very problematic for machine authentication in general. For this reason, features of this category are not addressed by the proposed check routines.

The 48 generic check routines defined below consist of so-called *basic check routines (BR)* and *composite check routines (CR)*. Basic check routines are individual routines, which refer to one property (e.g. IR absorption) of a single feature. Composite check routines are defined as logical combinations of basic check routines. Consequently, a single feature can be tested for multiple properties such as IR absorption and transparency in visible light.

For the basic check routines, the following abbreviated definitions according to [BSI-TR-03135] are used:

Basic check routine := (XX, YY, ZZ)

XX specifies the light source for the image on which the check routine is performed:

- **IR** – Infrared light
- **UV** – Ultraviolet light
- **VI** – Visible (white) light

YY is an identifier for the optical property of the particular feature:

- **AB** – absorbent, property of ink
- **BR** – brightness, property of substrate (e.g. bright under exposure of UV light)
- **FR** – spatial frequency property of patterns (e.g. characteristics of patterns obtained after spatial frequency transformation such as spatial Fourier transformation)
- **LU** – luminescent, property of patterns (e.g. visible under exposure of UV light)
- **TL** – translucent, property of ink shining through the substrate
- **TR** – transparent, property of ink (e.g. transparent under exposure of IR light)

ZZ is an identifier[7] for the feature itself or the position in the document:

- **FI** – Fibers
- **FU** – Full (complete) data page
- **IS** – printed feature, which already exists on the substrate (ink static)
- **MR** – Machine Readable Zone (MRZ)
- **OM** – Overprinted MRZ
- **CA** – Card Access Number (short: CAN)
- **BC** – Barcode feature
- **PD** – Personalized, “dynamic” perforation
- **PS** – Perforation showing “static” content

[7] Within this nomenclature, document model specific properties are denoted by “static” (such as UV overprint of a coat of arms) whereas document specific (individual/personalised) properties are denoted by “dynamic” (such as UV overprint repeating the document number).

- **PH** – Area of the photo
- **SP** – Area of the secondary photo
- **OP** – Overprinted photo
- **TH** – Security thread
- **VZ** – Visual inspection zone (VIZ)
- **WM** – Watermark
- **ID** – any other personalized, “dynamic” feature (ink dynamic), e.g. a secondary photograph
- **AF** – any additional feature that cannot be attributed to the items specified above

If a generic check routine consists of more than one single check routine, a sequential number has to be assigned to each single check routine.

The following generic check routines result from these short-terms[8]:

Check of material properties: (12 BR + 1 CR)

- **(IR, AB, PS)** → (IR, absorbent, static perforation): Check whether the static perforation is visible under IR light.
- **(IR, AB, TH)** → (IR, absorbent, thread): Check whether the security thread is visible under IR light.
- **(IR, AB, WM)** → (IR, absorbent, watermark): Check whether the watermark is visible under IR light.
- **(UV, BR, FU)** → (UV, brightness, full): Check for the brightness of the full data page under UV light.
- **(UV, BR, MR)** → (UV, brightness, MRZ): Check for the brightness in the MRZ area under UV light.
- **(UV, BR, PH)** → (UV, brightness, photo): Check for the brightness in the photo area under UV light.
- **(UV, BR, VZ)** → (UV, brightness, VIZ): Check for the brightness in the Visual Inspection Zone (VIZ) under UV-light
- **(UV, LU, FI)** → (UV, luminescent, fibers): Check for the presence of fibers which are luminescent under UV light.
- **(UV, LU, PS)** → (UV, luminescent, static perforation): Check whether traces of a static perforation are luminescent under UV light.
- **(UV, LU, TH)** → (UV, luminescent, thread): Check for the presence of a security thread which is luminescent under UV light.

[8] Check routines based on the AF feature are not explicitly listed, because they can be combined with each of the mentioned light source and optical property.

- **(VI, TR, TH) →** (VI, transparent, thread): Check whether the security thread is transparent under visible light.
- **(VI, AB, PS) →** (VI, absorbent, static perforation): Check whether a static perforation is visible under visible light.
- **(IR, AB, TH)** ° (**VI, TR, TH) →** (IR, absorbent, thread) in combination with (VI, transparent, thread): Check whether a security thread, which is visible under IR light, is transparent under visible light.

Check of printing technique properties: (8 BR + 2 CR)

- **(IR, AB, IS) →** (IR, absorbent, static ink): Check whether the ink of the static print is absorbent under IR light.
- **(IR, TL, IS) →** (IR, translucent, static ink): Check whether the ink on the back of the data page (usually the title page) is translucent under IR light and can be detected on the IR image of the data page.
- **(IR, TR, IS) →** (IR, transparent, static ink): Check whether the ink of the static print is transparent under IR light.
- **(UV, LU, IS) →** (UV, luminescent, static ink): Check whether the ink of the static print is luminescent under UV light.
- **(UV, LU, OM) →** (UV, luminescent, overprinted MRZ): Check whether the ink of the static print is luminescent in the MRZ area under UV light.
- **(UV, LU, OP) →** (UV, luminescent, overprinted photo): Check whether the ink of the static print is luminescent in the area of the photo under UV light.
- **(VI, AB, IS) →** (VI, absorbent, static ink): Check whether the ink of the static print is absorbent under visible light.
- **(VI, TR, IS)** → (VI, transparent, static ink): Check whether the ink of the static print is transparent under visible light.
- **(IR, TR, IS)** ° **(IR, AB, IS) →** (IR, transparent, static ink) in combination with (IR, absorbent, static ink): Check whether parts of the static print are absorbent in IR light, whereas other parts of the same feature are transparent in IR light.
- **(IR, TR, IS)** ° **(VI, AB, IS) →** (IR, transparent, static ink) in combination with (VI, absorbent, static ink): Check whether the ink of the static print is both transparent under IR light and absorbent under visible light.

Check of personalization properties: (28 BR + 3 CR)

- **(IR, AB, ID) →** (IR, absorbent, dynamic ink): Check whether the ink of the dynamic print is absorbent under IR light.
- **(IR, AB, MR) →** (IR, absorbent, MRZ B900 check): Check whether the MRZ is visible under IR light.
- **(IR, AB, CA) →** (IR, absorbent, CAN): Check whether the CAN is visible under IR light.
- **(IR, AB, BC)** → (IR, absorbent, barcode): Check whether the barcode is visible under IR light.
- **(IR, AB, PD) →** (IR, absorbent, dynamic perforation): Check whether a dynamic perforation is visible under IR light.
- **(IR, AB, PH) →** (IR, absorbent, photo): Check whether the photo is visible under IR light.

- **(IR, FR, PH)** → (IR, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.
- **(IR, AB, SP)** → (IR, absorbent, secondary photo): Check whether the secondary photo is visible under IR light.
- **(IR, TR, SP)** → (IR, transparent, secondary photo): Check whether the secondary photo is transparent under IR light.
- **(IR, TR, ID)** → (IR, transparent, dynamic ink): Check whether the ink of the dynamic print is transparent under IR light.
- **(IR, TR, PH)** → (IR, transparent, photo): Check for the transparency of the photo under IR light.
- **(UV, FR, PH)** → (UV, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.
- **(UV, LU, SP)** → (UV, luminescent, secondary photo): Check whether the secondary photo is luminescent under UV light.
- **(UV, LU, BC)** → (UV, luminescent, barcode): Check whether the barcode is luminescent under UV light.
- **(UV, LU, ID)** → (UV, luminescent, dynamic ink): Check whether the ink of the dynamic print is luminescent under UV light.
- **(UV, LU, PD)** → (UV, luminescent, dynamic perforation): Check whether marks of a dynamic perforation are luminescent under UV light.
- **(VI, AB, ID)** → (VI, absorbent, dynamic ink): Check whether the ink of the dynamic print is visible under visible light.
- **(VI, AB, MR)** → (VI, absorbent, MRZ): Check whether the MRZ is visible under visible light.
- **(VI, AB, CA)** → (VI, absorbent, CAN): Check whether the CAN is visible under visible light.
- **(VI, AB, BC)** → (VI, absorbent, barcode): Check whether the barcode is visible under visible light.
- **(VI, TR, BC)** → (VI, transparent, barcode): Check whether the barcode is transparent under visible light.
- **(VI, AB, PD)** → (VI, absorbent, dynamic perforation): Check whether a dynamic perforation is visible under visible light.
- **(VI, AB, PH)** → (VI, absorbent, photo): Check whether the photo is visible under visible light.
- **(VI, AB, SP)** → (VI, absorbent, secondary photo): Check whether the secondary photo is visible under visible light.
- **(VI, TR, SP)** → (VI, transparent, secondary photo): Check whether the secondary photo is transparent under visible light.
- **(VI, FR, PH)** → (VI, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.

- **(VI, AB, SP)** → (VI, absorbent, secondary photo): Check whether the secondary photo is visible under visible light.
- **(VI, TR, ID)** → (VI, transparent, dynamic ink): Check whether the ink of the dynamic print is transparent under visible light.
- **(IR, TR, ID)** ° **(VI, AB, ID)** → (IR, transparent, dynamic ink) in combination with (VI, absorbent, dynamic ink): Check whether the ink of the dynamic print is transparent in IR light as well as absorbent under visible light.
- **(IR, TR, SP)** ° **(VI, AB, SP)** → (IR, transparent, secondary photo) in combination with (VI, absorbent, secondary photo): Check whether the secondary photo is transparent in IR light as well as absorbent under visible light.
- **(VI, TR, BC)** ° **(IR, AB, BC)** → (VI, transparent, barcode): Check whether the barcode is transparent under visible light as well as absorbent under IR light.

The following composite check routine is defined jointly for the two inspection classes printing and personalization:

- **(IR, TR, IS)** ° **(VI, AB, IS)** ° **(IR, AB, ID)** → (IR, transparent, static ink) in combination with (VI, absorbent, static ink) in combination with (IR, absorbent, dynamic ink): Check whether the ink of the static print is both absorbent under visible light and transparent in IR light. In addition, a dynamically printed feature is visible under IR light at the same position.

The check routines specified above are not of equal value related to their inspection significance. For instance, the result of the check routine (VI, AB, ID) is not meaningful per se. Though it gains in crucial importance for counterfeit detection when it is combined with the check routine (IR, TR, ID).

Counterfeit-specific properties or features should be incorporated by inverting the logic of check routines: e.g. a specific configuration of imitated security fibers by printing should be checked for absence of this pattern (i.e. VI, TR, IS).

The following Table 0-1 gives an overview of the classification of the generic check routine system. The three components of the routines' identifiers – feature, light source and property – are grouped in a matrix. Row, column and the cell's content describe a generic basic check routine. The assigned inspection classes are marked by the colors green (material), blue (printing technique) and yellow (personalization).

Feature		Light source		
		VI	UV	IR
Fibers	FI		LU	
Full data page	FU		BR	
Static printed feature	IS	{AB. TR}	LU	{AB, TR, TL}
MRZ	MR	AB	BR	AB
Overprinted MRZ	OM		LU	
CAN	CA	AB		AB
Barcode	BC	{AB, TR}	LU	AB
Personalized perforation (dynamic)	PD	AB	LU	AB
Perforation on the substrate (static)	PS	AB	LU	AB
Photo	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Secondary Photo	SP	{AB, TR}	LU	{AB, TR}
Overprinted photo	OP		LU	
Security thread	TH	TR	LU	AB
Visual Inspection zone, VIZ	VZ		BR	
Watermark	WM			AB
Personalized dynamic feature	ID	{AB, TR}	LU	{AB, TR}
Additional feature	AF	{AB,BR,LU,TL,TR}	{AB,BR,LU,TL,TR}	{AB,BR,LU, TL,TR}

Table 0-1: Matrix representation of the generic basic check routines

Optical properties are abbreviated as follows: AB – absorbent, property of ink; BR – brightness, property of substrate; FR – spatial frequency, property of patterns; LU – luminescent, property of patterns; TL – translucent, property of ink shining through the substrate; TR – transparent, property of ink

Inspection classes are marked by the colors: green (material), blue (printing technique) and yellow (personalization).

C.4 RECOMMANDATIONS FOR MACHINE AUTHENTICATION OF MRTD'S

The following key components are involved in the process of automated machine authentication: the document, the full page reader and the authentication software (incl. the authentication database, see section C.2.2). However, these components are often designed/manufactured without consideration of their interdependencies especially with respect to the security-document design. In order to be able to perform an optimal machine authentication it is crucial that these components flawlessly interact with each other.

In the following sections, recommendations are given for efficient and effective design for the document itself (see section C.4.1), for the full page reader (see section C.4.2), for the authentication software (see section C.4.3), for the authentication database (see section C.4.4) and for the reference database (see section C.4.5). In section C.4.6, the recommendations made in the former sections are mapped to exemplary usage scenarios in order to support operational managers[9] in planning the operation of optical authentication systems.

When discussing recommendations for the different components, the difference of the typically involved time scales should be respected when referring to changes made:

- Inspection system software: 1 - 12 months
- Inspection system hardware: 3 - 5 years
- Security Document: 10 - 20 years (resulting from a typical issuing period of 5 – 10 years, and a validity period 5 – 10 years)

C. 4.1 Document Designers

To design a document with optical features as secure as possible for the human inspection should not be the only goal of a document designer. The security features offered by the document should be applicable for machine authentication as well. In addition to the base design of machine readable travel documents (MRTD's)according to ICAO Doc 9303, the following chapters summarize suitable features for machine authentication. Additionally, the following chapters will also summarize features that – even though they are of value for the human inspection – may counteract machine authentication (section 0). These features will be referred to as "potentially interfering" in the context of machine authentication.

Document designers should not be deterred from including those features in a document and should consider including those features while keeping their possible (negative) impact on the machine authentication process in mind.

C. 4.1.1 Suitable Features for Machine Authentication

In the following, recommendations concerning suitable features for machine authentication are listed. These features have been selected because they are easy to detect on VI, IR and UV images and at the same time increase the counterfeiting effort.

A.1 **Define unambiguous identification features:** It is a common practice among certain countries to bring out successive document models within a relative short period of time in order to improve the security properties of their MRTDs. The British passport models (GBR, P, 1, 2008) and (GBR, P, 2, 2010) are good examples of successive document models. It is therefore required, during the document design process, to define features, which enable an unambiguous identification of the document model (e.g. barcode[10] with document model).

[9] Operational manager: Organization responsible for the administration and the management of all processes related to the operation of the authentication infrastructure. The operational manager establishes and maintains communication channels with the vendors/manufacturers of the products used in the final authentication system.

[10] This example does not contradict the recommendations of Doc9303 (cf. section B3.6 of Doc9303 which are meant for storing biometric data.

A.2 **Define features under all three light sources:** Field experience has shown that it is quite challenging for counterfeiters to properly reproduce features which appear genuine under different light sources while it is a standard feature of full page readers to capture images under these light sources. The definition of optical security features under all three light sources (VI, IR and UV) is therefore required to significantly increase the effort required to produce counterfeits.

A.3 **Define features in three categories:** Providing a balanced distribution of security features in the classes “material”, “printing technique” and “personalization” also increases the counterfeiting effort. Therefore, features must be defined in each class in compliance to ICAO Doc 9303.

A.4 **Define features on both sides of ID cards:** ID-1 sized ID cards are allowed to be positioned on a full page reader with both sides. Hence, document designers shall design ID-1 sized ID cards with identification and verification features on both sides in order to allow identification and verification independent of the card side.

A.5 **Define features reacting differently under different light sources:** Document features behaving differently under different light sources (see Figure 0–4), help to considerably reduce the success probability of counterfeiters in producing proper counterfeits. For machine authentication, it is therefore required to use features that can be either checked for their presence and/or absence, depending on the corresponding light source (e.g. metameric inks, also called IR split in Figure 0–4, checkable by routine (IR, TR, IS) ° (VI, AB, IS)).

Figure 0–4: Passport (CZE, P, 1, 2011): IR split in title text

A.6 **Define features with different colors under UV light:** Features with different luminescent colors under UV light (see Figure 0–5) make the reproduction of that feature more complicated and are therefore recommended. At the same time, the color scheme of that feature can be checked during machine based authentication in addition to the simple presence check of that feature. Furthermore, it is recommended to use colors that differ significantly with respect to their chromaticity coordinates in order to facilitate the distinction by machines. The luminescence properties of the involved inks tend to degrade which further increases the challenge for reliable automatic detection.

Figure 0–5: Passport (GBR, P, 2, 2010): UV pattern with two colors[11]

A.7 **Define patterns with individual content, e.g. secondary facial image:** It is recommended to define individual patterns that can both be checked for their property and compared with already existing dynamic content on the data page. For instance, a secondary facial image can be compared with the primary facial image, and these two representations can have the same or different spectral properties. The list of following patterns with secondary facial images is meant to illustrate this recommendation but is neither complete nor is it meant to be an explicit recommendation for these specific features:

a) Secondary facial image as smaller repetition of the facial image which is visible under visible light and transparent under IR light (checkable by (VI, AB, ID) ° (IR, TR, ID)).

b) Optically variable ink (OVI) and diffractive optically variable image devices (DOVIDs) that are personalized e.g. with laser engraving or laser ablation (see Figure 0–6). The exemplary feature depicted in Figure 0–6 shows different colors under different viewing angles in visible light (first and second picture) and a secondary facial image slightly visible under transmitted light (third picture). Under IR light, the secondary facial image can clearly be captured and compared to the facial image. The feature is checkable by the following composite check routine: (IR, AB, ID) ° (VI, AB, IS) ° (IR, TR, IS), which is a threefold combination.

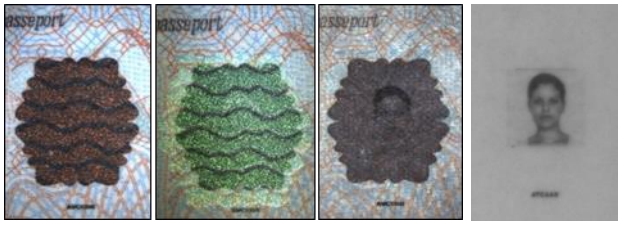


Figure 0–6: Passport (HUN, P, 1, 2006): Personalized OVI viewed under two different angles, under transmitted light and under IR light

[11] Source: http://edisontd.net/

c) Personalized laser engraving that reacts in an opposite (“negative”) manner (see Figure 0–7). The exemplary feature depicted in Figure 0–7 can be captured in visible light, where it shows a negative secondary facial image under two different angles.

Figure 0–7: Passport (LVA, P, 1, 2015): “Negative” personalization through laser engraving under different viewing angles in visible light

A.8 **Define features that remain stable over the validity period of the MRTD:** Some features tend to wear out over time. Colors of UV patterns, for instance, may fade over the validity period of the MRTD. Overlay glues can make UV patterns considerably lose their sharpness over time, leading to possible inaccurate check results for the feature. It is therefore recommended to define features that remain as stable as possible over of the validity period of the MRTD.

A.9 **Define a utopian document holder for specimen documents:** In order to establish a standardized way to identify specimen documents, it is recommended to set the nationality of the document holder to “UTO” for sample documents.

C. 4.1.2 Potentially interfering features for Machine Authentication

This section deals with features that can possibly interfere with machine authentication (within the context mentioned at the beginning of section C.4.1):

- **Overlapping features:** Overlapping features which are defined without considering their interdependency may negatively interact under the influence of a light source. The diffractive effects of a DOVID may interfere with the acquisition of the data page (see Figure 0–8).

Figure 0–8: Passport (AUT, P, 1, 2006): Hologram security laminate with optically distorting influence

- **Features near the upper edge of the document:** Field experience has shown that optical features close to the document upper edge (e.g. in case of an involved booklet) can interfere with machine authentication and may lead to cutting of the captured area. A partial capture of that feature might lead to errors.

- **Features only visible in high resolution:** Based on current state of technology, most of the current full page readers used in authentication systems support a maximal nominal resolution of 400 ppi providing real optical resolutions that are even below this value. Features which are only visible in high resolution of more than 400 ppi (e.g. microtext, Guilloches) will remain undetectable for most of the full page readers currently available on the market (see Figure 0–9). However, these features may be verifiable by full page readers in the near future having 600 ppi or more.

Figure 0–9: Passport (D, P, 1, 2017): Comparison between a high-resolution image of the microtext (1000 ppi) and an image of the same microtext taken from a full page reader (nominal 400 ppi)

- **Features for which the appearance depends on individual handling:** Some features are potentially not suited for machine authentication because they can considerably change the appearance of the document: depending on

how the page is placed on the document reader, the content of the live image is more or less different. In the following, two of such features are mentioned exemplarily:

a) Window feature: Depending on how data page and cover are placed on the document reader, it is possible to see the content of the cover through the window, the reader housing, the fingertip or the content of the window is empty (see Figure 0–10) leading to incident light.

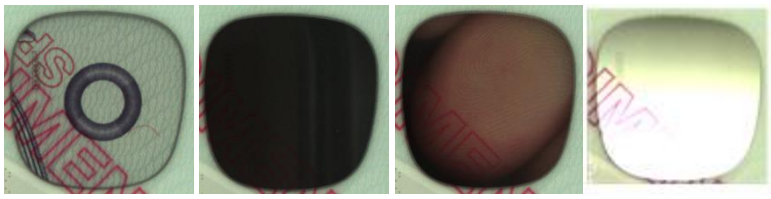


Figure 0–10: Passport (SWE, P, 1, 2012): Window feature with variable content; from left to right: inner front cover; reader housing; fingertip; glare induced by incident light

A single-sided window on ID-1 sized ID cards, i.e. a window feature that can be seen only from the front, is more suitable for machine authentication because the content of the window does not vary in the extent of Figure 0–10 and does not obstruct the checking process on the back of the card.

b) Transparent full page overlay sheet: These sheets can lead to different results depending on their presence (or absence) during the image capture process (see Figure 0–11).

Figure 0–11: Passport (BEL, P, 1, 2008); left: plain data page; right: data page with an overlay of the transparent sheet for visual inspection

The difficulties related to the use of these features can be overcome by proper training of the operator (in the case of human assisted document inspection) or user guidance (e.g. for automated border control).

- **Additional visa pages:** Passports that can be amended with additional visa page inserts can become too massive for ordinary full page reader geometries.

C. 4.2 Manufacturer of Full Page Reader

The reliability of an authentication process not only depends on the set of functionalities provided by the full page reader used in the process; a practical and easy handling of the deployed full page reader also has a direct impact on the quality of the images delivered to the authentication software (see Section C.4.3), and therefore automatically influences the overall result of the authentication process. The generic recommendations given in this section should be taken into consideration in the design process of full page readers:

C.1 **Assure proper wavelengths of light spectrum:** Image recording using proper wavelengths is a prerequisite for the appropriate analysis of optical features/properties. For example, a feature which is supposed to be transparent under IR light might become visible on an IR image if the capture is done with an inappropriate wavelength of the corresponding light spectrum. This might lead to faulty live data-sets, and therefore to a wrong interpretation of the optical check results. Following wave lengths for the corresponding light spectrums are required for recording images of live data-sets:

- VI: spectral range of 400 – 700 nm
- IR: a wavelength within the range of 850 – 950 nm[12]
- UV: 365 nm

Even though some passport readers support shorter UV wavelengths (e.g. 254 and 313 nm), this technology is still not widely spread yet and is not considered further in this document.

C.2 **Assure minimum resolution:** The quality of the live data-sets delivered to the authentication software, measured in pixel per inch (short: ppi), has a direct impact on the accuracy of the authentication process. Field experience has shown that live data-sets shall have a minimum resolution of 385 ppi [FRONTEX-ABC], although many properties of security printing would profit from an acquisition resolution of 600 ppi or higher.

C.3 **Deliver standard image formats:** Live data-sets shall be delivered in the most widely used/supported formats. As an example, the following formats can be used: BMP, JPG (incl. JPG2000) and PNG.

C.4 **Capture up to ID-3 size:** The full page reader should allow the verification of MRTDs of all sizes specified in Doc9303. The capture area should therefore be suitable for documents up to ID-3 size. Although this document focuses on full page readers, one should keep in mind that there are application scenarios that do not require the verification of MRTDs of all sizes but only require the full page reader to scan documents of a specific size (e.g. mobile devices).

C.5 **Assure capturing of all areas with the same quality**: The full page reader shall be able to capture the whole data page with constant image quality. This can for example be provided by a homogeneous illumination of the capture surface.

[12] This value was derived from the recommendations defined in Doc9303 Part 3.

C.6 **Assure short response time and constant intensity**: The light source used for the capture shall have a short response time and shall provide constant light intensity because any deterioration of the light during the authentication process might lead to the generation of unsuitable live data-sets.

C.7 **Assure constant image quality**: The light sources of full page readers of the same type might emit light differently due to production-related deviations. In addition, these light sources conditions of a full page reader may change their intensity over time. The full page reader shall therefore implement functionalities that help to compensate for deviations thus providing a constant image quality over time and regardless of the individual device being used. In the following, two examples are given in order to illustrate how this recommendation can be fulfilled:

a) The manufacturer provides functionalities to perform color management and additional calibration (e.g. by means of a calibration card) and customize the settings of the full page reader (e.g. brightness, exposure time).

b) The manufacturer provides in-built sensors allowing for the automatic compensation of deviations.

C.8 **Allow setting of UV light exposure by authentication software**: Different document models often require different UV light exposure in order to illuminate the document optimally. In this case, the UV light exposure information is stored in the authentication database. Therefore, the full page reader shall allow the setting of the UV light exposure via the authentication software through forwarding of UV settings stored in the authentication database (cf. section C.4.4.2, item D.8.).

C.9 **Allow capturing of multiple UV images**: The full page reader should support multiple images capturing with different exposure setting, e.g. for a combination of UV features showing a high contrast in luminescence (e.g. high dynamic range).

C.10 **Allow glare-free images**: Reflections may appear on the captured image and often cover biographical data or security features of the data page. Therefore, the images delivered by the full page reader should contain as little glare as possible. This can be realized by capturing multiple visible (white) light images from different angles or by using diffuse illumination.

C.11 **Provide mechanism to press the document flat onto the capture area**: As stated previously, the user-friendliness of the full page reader directly influences the efficiency and the speed of the authentication process. The full page reader should therefore provide mechanisms to mechanically press the document flat onto the window in order to allow proper captures of the document pages.

C.12 **Allow single-handed operation**: Additionally, single-handed operation of the reader should be possible and the reading process should be symmetric such that it can be operated by right- and left-handed users.

C.13 **Provide interactive user guidance**: Interactive user guidance not only increases the comfort of users operating the document reader, it also helps to significantly reduce the duration of the whole authentication process. User guidance is crucial especially for ABC-gates typically following a self-service approach: In contrast to stationary document control, the document authentication hardware is used by document holders themselves. Therefore, the document reader should be able to provide interactive user guidance. This can be realized by, for example, delivering a live-stream of the document placed on the capture surface indicating the progress of the image capture

(e.g. scanner metaphor). In this way, the user gets a direct feedback and can notice much faster if the document is placed correctly on the document reader or not.

C.14 **Provide hardware with a high degree of robustness**: Depending on the deployment scenario, full page readers are subject to various external conditions (incorrect handling, humidity, etc.). Over time, these external conditions can more or less damage key components (e.g. scratches on the capture surface) of the full page reader, thus accelerating wear or even breakage of the device. It is therefore recommended to equip the full page reader with robust hardware components.

B. 4.3 Manufacturer of Authentication Software

The following proposals are exemplarily based on the technical guideline [BSI-TR-03135] by the Federal Office for Information Security (BSI) as it currently provides the only public sector solution within this area. It is highly recommended to implement the authentication software in accordance with this guideline. The subsequent recommendations should rather be understood as an extension of [BSI-TR-03135].

Please consider the following technical recommendations for the authentication software:

C.1 **Enable processing of pre-recorded images:** The authentication software shall also work without hardware and must be able to process pre-recorded images (minimum requirements for the images are given in section C.4.2, items C.1, C.2 and C.3). This functionality is especially important for automated evaluation processes. It is however necessary to prevent the authentication software from processing pre-recorded images during productive operation, as this can be used as a potential attack vector. Therefore, the usage of the interface used to process pre-recorded images must be restricted to specific configurations (e.g. evaluation setup).

C.2 **Enable processing of images from different hardware sources:** The software shall be able to process images taken from at least two different full page readers without degradation of verification results. The manufacturer of the authentication software shall therefore provide a specification describing the properties of the images delivered to the authentication software (color space, contrast, etc.).

C.3 **Abstract GUI from authentication software and hardware**: The optical authentication process of an MRTD is most of the time accompanied by the electronic check of this MRTD and a biometric verification with the document holder’s face and maybe also the fingerprint. In addition, background checks, e.g. to SIS, have to be performed. Therefore, it is recommended to use an abstraction layer between the GUI and the concrete software and hardware components needed for document, biometric and background checks. In this way, the GUI is independent from these components. Furthermore, the mentioned components can be easily switched without changing the GUI.

In the following sections, the recommendations for manufacturers of authentication software products are structured in accordance with the steps executed during the process of authentication: The document must be detected (cf. section C.4.3.1), identified (cf. section C.4.3.2) and subsequently verified (cf. section C.4.3.3). Furthermore, the whole process must be visualized (cf. section C.4.3.4) and documented by using appropriate logging mechanisms (cf. section C.4.3.5).

C. 4.3.1 Document detection

For the detection of documents placed on the reader's surface, the following recommendations are given:

C.4 **Detect document automatically and manually**: The authentication software shall provide mechanisms for automatic and manual triggering of document detection. Manual triggering is especially crucial if automatic document detection does not operate properly.

C.5 **Compensate rotation and crop captured data page accordingly**: Image capturing is started automatically after the complete personal data page has been placed on the capture surface. The authentication software shall be able to compensate potential rotation and realign the image automatically. Additionally, the authentication shall crop the captured data page accordingly for further processing.

C.6 **Detect document based on optical presence**: The presence of a document shall be detected only by using its optical properties. The detection process shall still be carried out optically even if an expected chip is absent or malfunctioning (cf. section C.1.3).

C. 4.3.2 Identification

A prerequisite for document verification is the correct identification of the document model. For the identification of a live data-set, the following recommendations are given:

C.7 **Identify the document model:** As previously mentioned, the verification of a document presupposes a correct identification of its document. Therefore, it is required to identify to document model, regardless of the methods applied as long as the method applied guarantees a correct identification of the document model. The most common methods used for document model identification are MRZ (incl. pattern analysis) or pattern analysis only.

C.8 **Allow fast identification via MRZ:** If the MRZ is used as primary input for document model identification, the authentication software should implement methods and routines allowing for a fast identification process. In the following, two examples are given in order to illustrate how this recommendation can be fulfilled:

a) Begin with the capture of the IR image in order to extract the MRZ and derive the document model.

b) Because generating images in full resolution can be time-consuming, a fast IR-image capture for an early MRZ analysis can be run with a lower resolution than the minimum recommended for the IR image used for identification purposes.

C.9 **Provide fallback if MRZ is not readable under IR light:** An unambiguous identification of the document model should be possible by all means, as long as the document allows it. Even if the MRZ is not readable under IR light (not ICAO-compliant), the document has to be identified correctly. The software manufacturer therefore must support fallback solutions like performing OCR in the VI image for MRZ analysis if the MRZ is not printed using IR absorbent ink.

C.10 **Provide an unambiguous document model:** The software manufacturer must provide an unambiguous link to the document model in order to allow access to the authentication data-set of this document model in the authentication database.

C.11 **Enable partial identification:** The authentication software should enable partial identification to be configured in order to considerably reduce false identification and non-identification rates. Nevertheless, the assessment of partial identification requires human interaction and specific knowledge on MRTDs to select the correct document model manually and therefore does not suit every scenario, e.g. ABC gates.

C.12 **Enable manual identification:** The system should allow for a completely manual choice of the document model – instead of the automatic process and/or by overruling the machine's choice – for cases in which the system's automatic identification process fails. Furthermore, the system should only allow for manual identification if partial identification cannot be performed. Naturally, manual identification requires human interaction, specific knowledge on MRTDs and therefore does not suit every scenario (e.g. is not practical for ABC).

C.13 **Identify ID cards on both sides:** ID-1 sized documents are special in the sense that the MRZ is not on the personal data page (showing the facial image). However, ID-1 sized ID cards are allowed to be positioned on a full page reader with both sides. Therefore, ID-1 sized documents should be identifiable on either side of the document (cf. recommendation A.4 in section C.4.1.1).

C.14 **Identify specimen documents:** The authentication software should also identify sample or specimen-documents as such and inform the operator accordingly without interrupting the authentication process (cf. recommendation A.9 in Section C.4.1.1).

Recommendations for the visualization of the identification procedure in the graphic user interface can be found in section C.4.3.4.

C. 4.3.3 Verification

In the following, recommendations for verifying documents are given:

C.15 **Perform minimum number of spectrally selective checks:** Spectrally selective check routines must be performed in order to check the absorbent, reflective or luminescent reactions of the live data-set. Even if a document could not be identified, following mandatory checks must be performed:

a) (IR, AB, MR): this check routine also known as B900 test can be performed without selection of a document model, and

b) (UV, BR, FU): with certain restrictions on accuracy, this check routine can also be performed on non-identified live-datasets.

If the document model could be identified, the following spectrally selective checks complementary to the above mentioned (i.e. checking the optically opposite property) shall be performed additionally:

a) (IR, TR, *ZZ*): at least one check which investigates the complementary property "transparent under IR light" compared to (IR, AB, MR) shall be performed.

b) (UV, LU, *ZZ*): at least one check which investigates the complementary property "luminescent under UV light" compared to (UV, BR, FU) shall be performed.

C.16 **Perform MRZ consistency check:** Besides the minimum number of spectrally selective checks, plausibility checks (e.g. errors in MRZ, ICAO-3-Letter-Code) must be performed with all documents in order to guarantee minimal security also in case of non-identification.

C.17 **Perform checks in all categories**: The authentication software shall perform check routines in all three categories (material, printing technique and issuing technique) and cover all three light source images (cf. recommendation A.3 for document designers in section C.4.1.1).

C.18 **Verify chip presence**: If the existence of an RF chip is expected for a particular document model, which is not working or seems not existent, this must clearly raise a warning in addition to the optical results (cf. section C.1.3).

C.19 **Check dynamic patterns**: It is recommended to provide algorithms which compare individual respectively dynamic patterns (e.g. photo, signature). For instance, the facial image could be compared with a secondary facial image located on the data page (see Figure 0–12 and recommendation A.7 for document designer in section **Error! Reference source not found.**).

Figure 0–12: Passport (EST, P, 1, 2013): Verify the facial image in the visible light image against the one printed with UV-luminescent ink

C.20 **Combine check routines if necessary**: Some features can be checked by different check routines. For example, features behaving differently under different light sources serve as input for separate check routines (cf. recommendation A.5 for document designers in section C.4.1.1). It is therefore recommended to combine the results of such check routines logically or to combine the check scores by a decision function. For instance, a composite check routine could still output a pass-decision, even if the score of one basic check routine is slightly below its threshold.

C.21 **Perform redundant check routines on multiple positions:** For features which appear more than once on the document, the corresponding check routine should be also performed on multiple positions on the live data-set. For example, for the document model (D, P, 1, 2007) in Figure 0–13, the UV eagle-pattern can be checked on multiple positions. A check routine performed on multiple positions is called a redundant check routine.

Figure 0–13: Redundant pattern verification

In addition to multiple appearance of a feature, some features are statistically more subject to falsification than others. In many cases, counterfeiters for example change the date of expiry or substitute the facial image. It is therefore recommended to perform check routines, which are able to detect attacks on these “sensitive” features, redundantly.

C.22 **Perform redundant check routines on multiple UV colors:** Execution of redundant check routines is also recommended for UV features which appear in multiple colors on the document (cf. recommendation A.6 and Figure 0–5 for document designers in section C.4.1.1).

C.23 **Link and check both pages of an ID card:** A second page scan shall be linked automatically to the previous scan if both are from the same ID document. In addition, it is recommended to verify both sides of ID-1 sized documents in order to get an overall verification result for both sides, and maximize the number of optical features used for the authentication of the document (cf. recommendation A.4 for document designers in section C.4.1.1).

C.24 **Allow multiple pages cross checking of personal data:** Personal data of the document’s holder should be identical, regardless of the page on which they are. For instance, personal data on the data page of a passport are supposed to be identical to personal data on potentially existing visa. It is therefore recommended to perform multiple sides cross checks if e.g. personalized contents are expected to be identical / redundant.

C.25 **Perform check routines dependent on significance:** It is not always necessary or meaningful to perform a whole set of check routines just because it is technically possible to apply them on the live data-set. A more efficient approach would be to assess the relevance of the checks in correlation with the verification process. Some check routines are more susceptible to deliver helpful results than others, and deliver information leading to a more accurate analysis of the verification results. Therefore:

a) The checks should be conducted by their order of relevance/significance and the results immediately shown in the graphical user interface (see Visualization in section C.4.3.4), and

b) The results of the checks should be combinable by decision functions different from only performing a simple logical AND-combination (i.e. using weighted check results). Decision functions have to be logged in the XML catalogue (cf. recommendation C.46 for Logging in section C.4.3.5).

C.26 **Consider feature deviation**: Security features may change over time because of wear and tear of the MRTD, e.g. some UV colors may degrade. However, these features have to be checked with constant reliability during the MRTD validity period. Therefore, tolerances of check routines should be considered.

C.27 **Detect generic attacks:** In addition to the pure verification of document feature properties, the authentication software should provide tools for the detection of traces of generic attacks such as “paper damage”, “cut marks”, “photo substitution” or “laminate wrinkles” if the illumination conditions allow for it. The scheme for generic check routines can also be applied to checks detecting forgeries.

Recommendations for the visualization of the verification procedure in the graphic user interface can be found in the next section.

C. 4.3.4 Visualization

Visualization of the authentication results is the process by which the user of the authentication system is provided with visual feedback and information about the results of the authentication process. The visualization should be realized in the form of a graphic user interface (short: GUI).

The GUI for the visualization of optical check results should provide the user only with the most relevant information in order to be able to determine irregularities at first sight. In the following, this information is divided into the so-called “process summary area” (see C.29), the so-called “optical overview area” (see C.30) and more detailed information is shown in the so-called “optical details area” (see C.35).

Recommendations for choosing eligible information and displaying it in a compact and minimalistic way are made in the following:

C.28 **Display all document checks in one GUI**: The GUI may be an integral part of the delivered authentication software or be delivered and operated in a separate abstraction layer. Independent from this, it is recommended to display all types of performed checks (electronic, biometric, optical and background) in one GUI. This considerably reduces the effort of the system’s operator and facilitates the assessment of the check results due to a better overview of the process. Furthermore, special focus should be placed on occurring anomalies or irregularities (cf. recommendations C.41– C.45).

C.29 **Always show *process summary area*:** This area should show the overall result of the optical authentication and must be displayed to the user on the start page (see Figure 0–14 for exemplary stationary border control GUI). This area should always be visible to the user, independent of further selected details on specific verification results. The process summary area should show one overall result of the optical authentication with a traffic light symbol. Furthermore, the area should display a cropped facial image of the data page next to the facial image stored on the chip, if present.

Figure 0–14: Exemplary start page for stationary border control GUI

C.30 **Display *optical overview area* on start page:** This area shows an overview of the optical check routines and should be displayed to the operator on the start page.

a) This area should contain the following information (see Figure 0–14):

- The VI (visible light) image of the document per default. The operator staff should be able to change the default image to IR or UV, depending on the specific requirements.
- The personal data of the document holder contained in the MRZ: last name, first name, date of birth, sex, nationality and optional data.
- The document data: document type, document number, issuing State or organization, date of expiry and optional data.
- The extracted MRZ to allow comparison of the extracted MRZ with the MRZ printed on the document.
- A button to allow the manual triggering of the document reading process.

- A cropped facial image of the data page next to the facial image stored on the chip (if present, cf. section C.1.3) to allow easy detection of photo substitution.

b) It is also recommended to display following information in the optical overview area:

- The age of the document holder as well as the remaining validity period. This information can be recognized easier and faster by the operator than the dates contained in the MRZ.

C.31 **Select more details via one click:** From the optical overview area, the operator should click only once to get access to an additional page containing more details of the optical verification: the *optical details area* (see C.35) For instance, in the exemplary GUI in Figure 0–14, more details can be retrieved by clicking on the area “Document data”.

C.32 **Show results with traffic lights**: As specified in [BSI-TR-03135], the results of the optical check processes should be displayed using a traffic light system (e.g. red/green/yellow/grey lights). In addition to the color, the traffic lights should contain unambiguous symbols indicating the verification results (e.g. check, cross). This is especially important for users with red-green color blindness. Furthermore, the representation scheme should be the same for all areas of the GUI (e.g. negative results are all displayed with the same symbol and color).

C.33 **Provide result mapping according to TR-03135**: The traffic light system should provide a consistent mapping to the following verification results: **successful**, **failed**, **undetermined** and **not supported/not performed** defined in [BSI-TR-03135]. Table 0-2 gives an overview of the mapping used in this document. This mapping is based on [BSI-TR-03135] and should be used for practical implementations of the GUI.

Verification result	Traffic light color
Successful	green
Failed	red
Undetermined	yellow
Not supported/not performed	grey
Aborted	black

Table 0-2: Traffic light system mapping

C.34 **Provide minimalistic result mapping**: Alternatively, a minimalistic mapping consisting only of the colors green and red may be used for the traffic light system. As displayed in Table 0-3, the color green can be used to display a positive verification result, whereby the color red can be used to display any other verification result.

Verification result	Traffic light color
Successful	green
Failed	red
Undetermined	
Not supported/not performed	grey
Aborted	

Table 0-3: Minimalistic traffic light system mapping

A further reduction of the mapping would be to display the last four verifications in Table 0-3results with red.

C.35 **Display details in a dedicated *optical details area*:** The details area is only available via user click and contains detailed information about the different processes and results of the optical authentication. It is meant to provide the user with the information needed to perform further analysis if required.

a) The optical details area should contain the following information (see example in Figure 0–15):

- The VI, the IR and the UV image of the document. The three images should be presented next to each other.
- The proprietary document model identifier of the manufacturer of the authentication software, if the document model identifier proposed in section C.2.1 cannot be displayed in generic form.
- A list of selected check routines, showing their results via traffic lights: In the context of border control, the border control guard should only be confronted with the most important verification information in a human readable form. Therefore, the results of the generic check routines are summarized in three categories, described by easy and understandable terms
  - MRZ IR readability: The corresponding traffic light shows the result of the generic check routine (IR, AB, MR).
  - UV brightness: The corresponding traffic light shows the combined result of the generic check routines (UV, BR, FU), (UV, BR, VZ), (UV, BR, PH) and (UV, BR, MR).
  - Pattern check: The corresponding traffic light shows the combined result of the remaining generic check routines which have been performed for this document (see section 0).
- In addition, the results of the following mandatory checks according to [BSI-TR-03135] should be visualized using traffic lights:
  - MRZ consistency

- Date of expiry

- The extracted MRZ.

- During the authentication process, the data elements extracted from the optically read MRZ are compared with the MRZ elements stored on the chip (if available). The data elements of the optical MRZ should be displayed with the result(s) of this comparison. The result(s) should be displayed with the same traffic light system used throughout the GUI.

b) It is also recommended to display the following information in the optical details area:

- The identified document model in human readable form, e.g. D 2007. Using the standard document model identifier of [BSI-TR-03135] could probably cause more confusion than clarity amongst the users of the GUI. The representation of the document model identifier in the GUI should therefore be specified on the basis of common agreement with the operator of the authentication system.

- Both the data elements extracted from the optically read MRZ and the ones extracted from chip should be displayed next to each other (cf. section C.1.3).

Figure 0–15: Exemplary view for the optical details area

C.36 **Guide users during document reading**: During the reading process, the user should be given a hint to not remove the document before the reading process is complete (cf. recommendation C.13 in section C.4.2). For example, this hint can be realized as a process indicator displayed during the reading process. This hint can be placed upon the process summary area.

C.37 **Display information from central databases:** If the authentication process requires queries to a background database system, the optical details page may show the information retrieved from this system if it is correlated to optical authentication, e.g. the facial image retrieved from the central visa information system (C-VIS).

C.38 **Provide homogenous layout for MRTDs**: The layout of the GUI should be the same for all types of machine readable documents (e.g. passports, national ID cards, resident permits, etc.). For instance, the optical authentication information obtained from both sides of an ID-1 card should be displayed analogous to the visualization of the passport verification (one process summary area, one optical overview area and one optical details area).

C.39 **Guide operators through multi-page verification:** The verification of both sides of an ID-1 sized document demands an interactive guidance of the user. For a card put on the capture surface, the user should get a hint that the presentation of the second page could be the next step.

C.40 **Allow comparison of passport and visa/electronic residence permit (eRP) content:**

a) Guide operators through multi-page verification: During the verification of a passport, the user should be warned that the passport holder requires a visa/eRP in order to cross the border. This can, for example, be realized with a prompt on the overview page. This prompt should be an indication for the user, that the presentation of the visa/eRP to the full page reader is a possible next step.

b) Keep passport information available: During optical visa/eRP authentication, the overview and details areas showing the passport authentication results must still be available to be able to switch to them if desired.

c) Allow comparison in process summary area: Besides the optically captured facial image from the data page, the facial image on the visa/eRP should be displayed (see example in Figure 0–16). In addition, the chip image of the passport holder (if available, cf. section C.1.3) and the image retrieved from a visa information query system (e.g. the European VIS) or from the eRP chip should be displayed (see C.37).

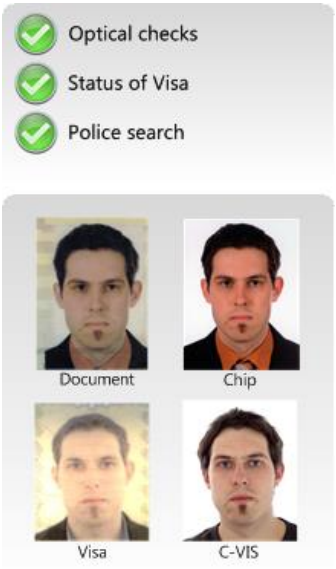


Figure 0–16: Exemplary view for the comparison of passport and visa

d) Allow comparison in visa optical details area: During the authentication process, the data elements Last Name, First Name, Date of birth, Sex and Nationality extracted from the optical MRZ of the visa are compared with these MRZ elements on the data page of the passport and/or the chip (cf. section C.1.3). The data elements of the visa MRZ should be displayed with the result(s) of this comparison. The result(s) should be displayed with the same traffic light system used in the rest of the GUI. The age of the document holder as well as the remaining validity period of the visa should also be displayed in this area, because this information can be recognized easier and faster by the operator than the dates contained in the MRZ.

In the following, recommendations for displaying errors are made:

C.41 **Highlight only irregularities**: It is required to make use of color highlighting only to signalize irregularities in the authentication process (e.g. example for check failure in Figure 0–14). This approach considerably helps the user in recognizing the most relevant information delivered by the GUI at first sight.

C.42 **Display errors in process summary area:** If a document is not authentic, the traffic light for the optical authentication must show a negative overall result. If the document model could not be identified, the traffic light for the overall optical authentication result should show a warning.

C.43 **Display errors in optical overview area:** If errors occur because of optical irregularities, they should be displayed in the following way:

a) Irregularity of spectrally selective property: If an error occurs because of a spectrally selective check routine, the image in the corresponding light spectrum should be displayed in the optical document data area instead of the standard VI image (e.g. if (UV, BR, FU) fails, the UV image should be displayed). In addition, the optical overview area should be surrounded by a red frame.

b) MRZ not consistent: If an error occurs because of the MRZ consistency check, the corresponding part of the extracted MRZ including the check sum should be highlighted in red. In addition, the corresponding inconsistent personal data and the area containing the personal data should be highlighted in red (e.g. see Figure 0–17). The operator should be able to manually correct the MRZ and trigger another reading process manually via a button.

Figure 0–17: Exemplary view for error visualization: MRZ consistency

c) Document expired: If the document is expired, the date of expiry should be highlighted red.

d) Chip not detected: If an electronic chip is expected in the identified document model but it cannot be detected (cf. section C.1.3), a warning should be displayed. The warning symbol should clearly be distinguishable from the traffic light symbols used to display the check results (e.g. yellow triangular warning sign).

C.44 **Display errors in optical details area:** If errors occur because of optical irregularities, they should be displayed in the following way:

a) Document not identified: If the document model could not be identified, a warning symbol should be displayed as result of the document model identification. The warning symbol should be clearly distinguishable from the traffic light symbols used to display the check results (e.g. yellow triangular warning sign, see Figure 0–18). A warning text should be displayed next to the warning symbol, e.g. “Document model could not be identified”.

b) Negative verification check: For every verification check displayed in the details page (see Figure 0–18), a negative check result should lead to a red traffic light. The respective features of the failed spectrally selective check should be highlighted on the corresponding image, e.g. by showing a red rectangle surrounding the searching area of the feature (e.g. the MRZ of the IR image due to a negative MRZ IR readability).

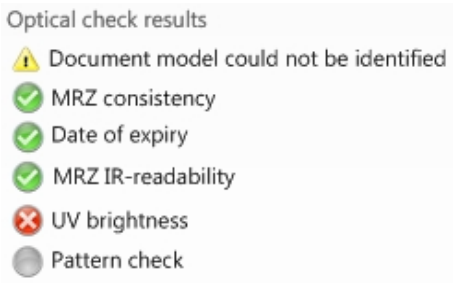


Figure 0–18: Exemplary for view error visualization: Document model and negative verification check

c) Inconsistent chip information: For every MRZ data which is not the same for the optical data page and the chip (cf. section C.1.3), the inconsistent pair of information should be displayed in red (with a warning symbol, see Figure 0–19).

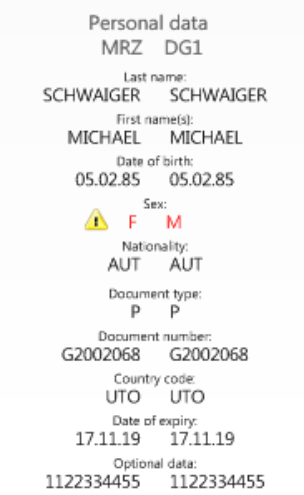


Figure 0–19: Exemplary view for error visualization: MRZ data

d) Inconsistent overall check digit: Errors related to the overall check digit (cf. Doc9303) could be an indication for a manipulation of the check digits, e.g. insertion of incorrect check digits in the MRZ in order to prevent the execution of access control mechanisms (e.g. BAC). For every failed check on the optical MRZ, the captured check digit of the corresponding MRZ element should be displayed next to the expected check digit.

C.45 **Display errors of passport and visa/eRP comparison:** If at least one of the comparable MRZ data is not the same for the passport and the visa/eRP, this inconsistency should be displayed in the following way:

a) Visa/eRP overview area: The comparable MRZ data (Last Name, First Name, Date of Birth, Sex, and Nationality) of the passport must be displayed in the visa/eRP overview page next to the MRZ data of the visa/eRP. Every inconsistent pair of information should be displayed in red with a warning symbol (see example in Figure 0–20).

Figure 0–20: Exemplary view for the comparison of the visa and the passport data

- Visa/eRP details area: For every MRZ data which is not the same for the visa/eRP and the passport, the inconsistent pair of information should be displayed in red (with a warning symbol).

C. 4.3.4 Logging

For the logging of the optical machine authentication process, the following recommendations are applicable:

C.46 **Log XMLs according to TR-03135:** Logging must be realized according to the XML schemes defined in [BSI-TR-03135] which contain, besides the detailed optical results, also the results of the electronic and combined (optical and electronic) verification of a document. For instance, this allows to:

- Log the generic check routine identifier of a proprietary check routine (see section 0).
- Put check routines in silent mode, i.e. the routine is executed and its results are logged, but the check result is not taken into account in the overall result of the authentication process. This is of particular importance if new check routines, algorithms or thresholds are evaluated.

Further information on the spectrally selective checks might be required by the operator for evaluation purposes and to update the underlying database to guarantee consistent and high quality authentication results over time. This information is the same for all documents of a specific document model, for example the decision function, textual explanations on the check routines, the image section from the reference database etc. Therefore, the manufacturer must supply this XML catalogue in machine readable form according to the defined XML scheme in [BSI-TR-03135] which summarizes all necessary information on the spectrally selective verification checks. Due to the format, the catalogue can be integrated into the evaluation of the results.

C.47 **Allow logging of optional image data:** The XML schemes defined in [BSI-TR-03135] allow but not directly regulate the storage of the processed live data-set as well as cropped images displaying the search area of check routines. The authentication software must be able to store the mentioned image data in the XML data strucutre. Recommendations for the operational manager for storing image data in compliance with the prevailing data protection regulations are made in section 0.

C.48 **Provide anonymization capabilities:** The software should provide capabilities to anonymize the live data-set directly after the authentication in order to be allowed to permanently store the images for further inspection. Please refer to section C.5.1 for recommendations for anonymization.

C. 4.4 Manufacturer of the Authentication Database

As described in section C.2.1 and C.2.2, the authentication database contains distinct sets of check routines for different document models. It directly interacts with the authentication software to which it delivers the set of check routines corresponding to the identified document model. Because of new established document models and permanently arising counterfeits, a well-maintained, flexible authentication database is crucial. In the following sections, the recommendations for the database are summarized concerning the updating process (see section C.4.4.1) and the configurability of the database (see section C.4.4.2).

C. 4.4.1 Update

The following recommendations are given for manufacturers of authentication databases regarding the update process:

D.1 **Exchange information about new document models or counterfeits**: The manufacturer of the authentication database shall establish a dedicated communication channel with the operational manager for secure transfer of datasets with information on new document models that should be inserted in the database. The manufacturer shall exchange information about new document models with the operational manager by using one of the following method:

a) Exchange via original sample: In this case, an original sample of the new document model or the counterfeit must be provided for definition and upload of the corresponding set of check routines in the database. The established communication channel and associated processes must take into account national legislation on data protection (cf. section 0).

b) Exchange via capture software: In this case, capture software has to be provided to the operational manager in order to generate a suitable live data-set of new document models or counterfeits. This data-set must at least contain one VI, UV and IR image. Ideally, several images of one light spectrum should be generated by this capture software (analogous to high dynamic range photography). The data-set is transferred to the manufacturer for definition of a corresponding set of check routines to be included in the next edition of the database. The manufacturer must recommend a list of suitable capture devices for this purpose.

D.2 **Update database regularly**: The authentication database shall enable regularly scheduled updates (minimum every 3 months). The authentication database shall also enable ad hoc updates on special (urgent) request:

a) If the manufacturer obtained new information about genuine documents or counterfeits and updated the document database based on this information in cooperation with the operational manager (see D.1 a), or

b) If the operator generated a live data-set with the capture software (genuine document or counterfeit) and sent it to the manufacturer (see D.1 b).

D.3 **Provide incremental updates**: By default, the manufacturer of the authentication database must supply the operator with full version updates. Incremental updates should also be distributed in order to save time and bandwidth.

D.4 **Provide sufficient documentation on changes**: At update delivery, the manufacturer of the authentication database must provide sufficient documentation about the changes made in the database.

C. 4.4.2 Database content and configurability

In this section a list of recommendation for manufacturers of authentication databases regarding the content and configurability of the database are given:

D.5 **Provide reduced content scales:** The authentication database should be available with different scales and therefore customizable for different scenarios. For instance, commercial scenarios are much limited in scope and the type of checked documents is generally very specific (e.g. document authentication at car rental companies). It is therefore recommended to provide authentication databases that specifically address the needs of commercial scenarios via reduced content scales. By providing a database with reduced scales, the manufacturer ensures that it remains cost efficient and easy to integrate in different setups.

D.6 **Allocate checks with significance levels**: Checks should be allocated with a significance level to allow the authentication software to perform the checks in order of significance (see recommendation C.25 a) for manufacturer of authentication software in section C.4.3).

D.7 **Provide different operational modes**: Different usage scenarios require different levels of security concerning the acceptance or rejection of a document: Stationary border control, for instance, relies on high security, whereas commercial scenarios focus in general more on high convenience for the document's holder. Therefore, the authentication database should provide at minimum two different operational modes for high security and for high convenience.

D.8 **Provide document model specific UV light exposure information**: As mentioned in section C.4.2, different document models often require different UV light exposure. For example, certain document models require a longer UV illumination in order to properly check specific features under UV light. Therefore, the authentication database should contain information about the UV exposure settings required for corresponding document models, so that the authentication software can automatically configure the full page reader accordingly (cf. section C.4.2, item C.8).

D.9 **Support server-based setup**: It is recommended to supply an authentication database that can also be operated in a server-based setup. In this case, different authentication software would be able to access a single authentication database. Additionally, two or more authentication databases could be operated as a cluster being accessible for several authentication software products.

B. 4.5 Manufacturer of the Reference Database

Even though the reference database is not directly a part of the authentication system (see Section C.2.1) it can be used as a complementary source of information if the authenticity of a document cannot be clearly determined on basis of the machine authentication. In this case, the reference database is able to support the operator with detailed information on the corresponding document model, e.g. with high quality images of features, textual explanations and information on common counterfeits (aimed for 2nd-line / back-office inspection). An example for a reference database provided by the European Union is the so-called FADO system (False and Authentic Documents Online). The publicly available counterpart of the FADO is the so-called PRADO[13] (Public Register of Authentic Documents Online).

In case of its usage, there are some practical implications that need to be considered by the manufacturer of the reference database. This section addresses these implications in the form of recommendations:

E.1 **Provide automatic output:** The reference database shall receive and process an unambiguous link to a document model as input from the identification process. It should also provide a reference data-set corresponding to the link as output.

E.2 **Allow manual selection of data set**: In addition to the automatic selection of a reference data-set, an operator shall also be able to manually search for and choose a specific data set via a GUI.

E.3 **Provide extensive information on authentic documents**: The reference database shall contain information on authentic documents and may be accompanied by linked descriptions of typical forgeries. Specific properties of the reference document models shall be described in detail and every content shall have a textual description.

In this context it is worth mentioning that a database such as EDISON-TD can also be taken into consideration. In order to increase the usage of commercial databases, the mechanisms described in recommendation D.1 can be used.

C. 4.5 Operational Manager

The so-called *operational manager* is the organization responsible for the administration and the management of all processes related to the operation of the authentication infrastructure. Operators are members of the operational manager's staff who directly interacts with the authentication system.

The concrete realization of the planned operation depends on the inspection scenario. Exemplary scenarios are:

- **Stationary border control** (in short SBC): In this case, governmental customers for stationary border control assume the role of the operational manager (e.g. border police). Usually for this setup, operators are very familiar with optical document verification. The inspection scope is immense due to the high number and diversity of the checked documents. Furthermore, the system requires an extensive interaction and assessment of the operators who directly interact with both the system and the document's holder.

- **Automated border control via ABC gates** (in short ABC): For this scenario, governmental customers for ABC gates also assume the role of the operational manager which often more focus on fast than on extensive document authentication. The operators in this case are also well trained border guards and usually supervise a set on ABC-

[13] http://prado.consilium.europa.eu/en/homeindex.html.

gates valuing a minimalistic visualization. In contrast to stationary border control, the system is used by travelers and therefore needs extensive user guidance, which is out of scope of this paper.

- **Document authentication for commercial purposes** (in short CP): In this case, commercial customers assume the role of the operational manager (e. g in banks). Contrary to the previous mentioned scenarios, the operators are usually not familiar with optical document verification and the inspection scope is generally smaller than for border control.

The capabilities of the components acquired must be in line with the needs of the operational manager and the requirements of the deployment scenario. In this section, the recommendations for the manufacturers of full page readers (see section C.4.2), of authentication software (see section C.4.3), of authentication databases (see section C.4.4) and of reference databases (see section C.4.5) are mapped to the usage scenarios. Recommendations for monitoring in compliance with data protection regulations are made in chapter C.50.

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of full page readers.

Manufacturer of Full Page Readers				
		Usage scenario		
No.	Short description	SBC	ABC	CP
C.1	Assure proper wavelengths of light spectrum	X	X	X
C.2	Assure minimum resolution	X	X	X
C.3	Deliver standard image formats	X	X	X
C.4	Capture up to ID-3 size	X	X	X
C.5	Assure capturing of all areas with the same quality	X	X	X
C.6	Assure short response time and constant intensity	X	X	X
C.7	Assure constant image quality	X	X	
C.8	Allow setting of UV light exposure by authentication software	X	X	
C.9	Allow capturing of multiple UV images	X		
C.10	Allow glare-free images	X	X	
C.11	Provide mechanism to press the document flat onto the capture area	X	X	X
C.12	Allow single-handed operation	X	X	X

Manufacturer of Full Page Readers				
		Usage scenario		
No.	Short description	SBC	ABC	CP
C.13	Provide interactive user guidance		X	X[15]
C.14	Provide hardware with a high degree of robustness	X	X	X

Table 0-4: Recommendations for full page readers classified by inspection scenarios

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of authentication software products.

Manufacturer of Authentication Software				
		Usage scenario		
No.	Short description	SBC	ABC	CP
C.1	Enable processing of pre-recorded images[16]	X		
C.2	Enable processing of images from different hardware sources	X	X	X
C.3	Abstract GUI from authentication software and hardware	X	X	X
Document detection				
C.4	Detect document automatically and manually	X	X[17]	
C.5	Compensate rotation and crop captured data page accordingly	X	X	X
C.6	Detect document based on optical presence	X	X	X
Identification				
C.7	Identify the document model	X	X	X
C.8	Allow fast identification via MRZ	X	X	X
C.9	Provide fallback if MRZ is not readable under IR light	X	X	X

[15] The way user guidance is realized highly depends on the commercial use case.

[16] This recommendation is important for evaluation of authentication software products.

[17] Manual document detection is not applicable in the automated border control scenario.

Manufacturer of Authentication Software		Usage scenario		
No.	Short description	SBC	ABC	CP
C.10	Provide an unambiguous document model	X	X	X
C.11	Enable partial identification	X		
C.12	Enable manual identification	X		
C.13	Identify ID cards on both sides	X	X	X
C.14	Identify specimen documents	X	X	X
Verification				
C.15	Perform minimum number of spectrally selective checks	X	X	X
C.16	Perform MRZ consistency check	X	X	X
C.17	Perform checks in all categories	X	X	X
C.18	Verify chip presence	X	X	X
C.19	Check dynamic patterns	X	X	X
C.20	Combine check routines if necessary	X	X	X
C.21	Perform redundant check routines on multiple positions	X		X
C.22	Perform redundant check routines on multiple UV colors	X		
C.23	Link and check both pages	X	X	X
C.24	Allow multiple pages cross checking of personal data	X	X	X
C.25	Perform check routines dependent on significance	X	X	X
C.26	Consider feature deviation	X	X	X
C.27	Detect generic attacks	X	X	X
Visualization				
C.28	Display all document checks in one GUI	X	X	X

Manufacturer of Authentication Software				
		Usage scenario		
No.	Short description	SBC	ABC	CP
C.29	Always show *process summary area*	X	X	X
C.30	Display *optical overview area* on start page	X		
C.31	Select more details via one click	X	X	
C.32	Show results with traffic lights	X	X	X
C.33	Provide result mapping according to TR-03135	X	X	X
C.34	Provide minimalistic result mapping	X	X	X
C.35	Display details in a dedicated *optical details area*	X		
C.36	Guide users during document reading	X	X	X
C.37	Display information from central databases	X		
C.38	Provide homogenous layout for MRTDs	X		X
C.39	Guide operators through multi-page verification	X		
C.40	Allow comparison of passport and visa/electronic residence **permit (eRP) content**	X		
C.41	Highlight only irregularities	X	X	X
C.42	Display errors in process summary area	X	X	X
C.43	Display *optical overview area* on start page	X		
C.44	Display errors in optical details area	X		
C.45	Display errors of passport and visa/eRP comparison	X		
Logging				
C.46	Log XMLs according to TR-03135	X	X	X
C.47	Allow logging of optional image data	X	X	X

Manufacturer of Authentication Software				
		Usage scenario		
No.	Short description	SBC	ABC	CP
C.48	Provide anonymization capabilities	X	X	X

Table 0-5: Recommendations for authentication software classified by inspection scenarios

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of authentication databases.

Manufacturer of Authentication Database				
		Usage scenario		
No.	Short description	SBC	ABC	CP
D.1	Exchange information about new document models or counterfeits	X	X	
D.2	Update database regularly	X	X	X
D.3	Provide incremental updates	X	X	X
D.4	Provide sufficient documentation on changes	X	X	X
D.5	Provide reduced content scales			X
D.6	Allocate checks with significance levels	X	X	X
D.7	Provide different operational modes	X	X	X
D.8	Provide document model specific UV light exposure information	X	X	X
D.9	Support server-based setup	X	X	X

Table 0-6: Recommendations for authentication databases classified by inspection scenarios

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of reference databases.

Manufacturer of Reference Database				
		Usage scenario		
No.	Short description	SBC	ABC	CP
E.1	Provide automatic output	X		
E.2	Allow manual selection of data set	X		X[18]
E.3	Provide extensive information on authentic documents	X		X[18]

Table 0-7: Recommendations for reference databases classified by inspection scenarios

[18] Considering CP, it is important to adjust the level of knowledge, depending on the use case.

C.5 MONITORING IN COMPLIANCE WITH DATA PROTECTION

An optical authentication process may lead to an unexpected result due to one of the following reasons:

- A counterfeit has been detected.
- A counterfeit has been classified as authentic.
- An authentic document has been classified as counterfeit.
- A handling error of the full page reader occurred, e.g. the document has been removed from the reader during authentication.
- The document model could not been identified.

In these cases, it is crucial for the operational manager to be able to analyze the reason for the wrong decision. For this, the information gained in the authentication procedure - maybe including personal information - has to be logged and analyzed. This directly raises data protection issues, because personal data is not allowed to be stored, even encrypted, without the consent of the document's holder or a determined reason. The following recommendations can be made for the operational manager:

F.1 **Log authentication reporting**: Reporting information of the authentication procedure without personal data (e.g. identified document model, authentication results, check routine results etc.) must be logged according to [BSI-TR-03135]. The live data-set, the MRZ and the VIZ are therefore excluded from logging. Reporting information does not underlie any time restriction and can be used for statistical analyses.

F.2 **Set up feedback loop to manufacturer**: Regular feedback from the operation can be used to optimize the authentication software. Therefore, the reporting information clarified in F.1 should be forwarded to the manufacturer of the authentication software regularly.

F.3 **Store unaltered live data-set if eligible**: Analysis of errors can be done at its best on the same live data-set which has been provided for authentication. It is therefore recommended to store unaltered live data-sets in the XML scheme defined by [BSI-TR-03135] if this can be done with eligible effort and consent to data privacy concerns. The following logging possibilities including images exist:

a) Store live data-set with consent of document holder: If the scenario allows for it, the live data-set used for authentication can be stored, if the consent of the document holder has been collected first in written form. This way is only conceivable for scenarios allowing a communication with the document holder such as pilots and not for permanent operation. Furthermore, the live data-sets have to be deleted irretrievably after a contractually defined time period.

b) Store live data-set in case of error: Personal data is allowed to be stored for a contractually defined time period, if a determined reason for the storage exists, e.g. if an error occurred during authentication. If the

scenario allows for it, this time period can be used for error analysis on the unaltered live data-set, which have to be deleted irretrievably afterwards.

c) Log privacy friendly regions: To avoid data privacy concerns and at the same time preserve rough analysis possibilities, only “privacy friendly” cropped images displaying the search area of check routines can be logged. These regions of interest must not contain the whole facial image, the MRZ or the VIZ and can be stored for all authentication processes with no time restriction in the XML scheme defined by [BSI-TR-03135].

F.4 **Anonymize images if eligible:** Another proposition to avoid data privacy concerns but store the complete live data-set with no time restriction is to anonymize the personal data on the live data-set. Via this, the areas containing personal data are difficult to analyze whereas non-personal-related parts of the document remain fully analyzable. **Clarify data privacy concerns**: The data privacy concerns mentioned in recommendations F.1 to F.1 must be clarified by the operational manager, e.g. via a data privacy concept. Recommendations for storing the live data-set made in F.3 and F.1 can be combined, e.g. store privacy friendly regions.

C.6 BIBLIOGRAPHY

[BSI-TR-03135] BSI, Machine Authentication for Public Sector Applications, TR-03135,“ 2017. url: https://www.bsi.bund.de/tr03135/

[FRONTEX-ABC] FRONTEX: Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, 2012

— — — — — — — —

APPENDIX D TO PART 2 — THE PREVENTION OF FRAUD ASSOCIATED WITH THE ISSUANCE PROCESS (INFORMATIVE)

D.1 SCOPE

This Appendix describes the fraud risks associated with the process of MRTD application and issuance. These risks are a consequence of the benefits that can accrue from the possession of an MRTD that can be used to confirm the identity and citizenship of the holder. The Appendix recommends precautions that an issuing State can take to prevent such fraud.

D.2 FRAUD AND ITS PREVENTION

Fraud perpetrated as part of the issuance process can be of several major types:

- theft of genuine blank MRTDs and completion to make them look valid;
- applying for the MRTD under a false identity using genuine evidence of nationality and/or identity stolen from another individual, or otherwise obtained improperly;
- applying for the MRTD under a false identity using manufactured false evidence of nationality and/or identity;
- using falsely declared or undeclared lost and/or stolen MRTDs that can be provided to people who might use them in look-alike fraud or with repetitive photo substitutions; and
- reliance on MRTD employees to manipulate the MRTD system to issue an MRTD outside the rules.

There are two additional categories in which the applicant applies under his own identity but with the intention to be complicit in the later fraudulent use of the MRTD by:

- altering a genuinely issued document to make it fit a bearer who is not the person to whom the MRTD was issued; and
- applying for an MRTD with the intention of giving or selling it to someone who resembles the true bearer.

D.3 RECOMMENDED MEASURES AGAINST FRAUD

To combat the above-mentioned threats, it is recommended that the MRTD-issuing authority of the State undertake the following measures, to the extent that adequate resources are available for their implementation.

A suitably qualified person should be appointed to be Head of Security directly responsible to the Chief Executive Officer of the issuing authority. The Head of Security should be responsible for ensuring that security procedures are laid down,

observed and updated as necessary.

In each location where MRTDs are issued there should be a designated Security Manager. The Security Manager should be responsible for the implementation and updating of the security procedures and report directly to the Head of Security.

Vetting procedures should be established to ensure that all staff are recruited only after searches have verified their identity, ensured that they have no criminal record, and verified that their financial position is sound. Regular follow-up checks should also be made to detect staff whose changed circumstances mean they may succumb to temptations to engage in fraudulent activity.

All staff within the MRTD-issuing authority should be encouraged to adopt a positive attitude toward security matters. There should be a system of rewards for any staff member who reports incidents or identifies measures that prevent fraud.

Controls should be established that account for key components such as blank books and security laminates. Such items should each bear a unique serial number and should be kept locked in suitable secure storage. Only the required number should be issued at the start of each working day or shift. The counting of the items should be done and the agreed by two members of staff who should also record the unique numbers of the items. The person to whom they are issued must account for all items at the end of the shift in the form of either personalized documents or defective product. All items should be returned to the secure store at the end of the working period, again having been counted by two people and the unique numbers logged. The records should be kept at least for the life of the issued MRTDs.

Defective product or materials should be destroyed under controlled conditions and the unique numbers recorded.

The issuance process should be divided into discrete operations that are carried out in separate locations within the facility. The purpose is to ensure that no one person can carry out the whole issuance process without venturing into one or more areas that the person has no authorization to enter.

D.4 PROCEDURES TO COMBAT FRAUDULENT APPLICATIONS

The following procedures are recommended to prevent the issue of a genuine MRTD as a result of receipt of a fraudulent application.

The MRTD-issuing office should appoint an appropriate number of anti-fraud specialists (AFS) who have received a high level of training in the detection of all types of fraud used in MRTD applications. There should be at least one AFS present in each location in which MRTD applications and applicants are processed. An AFS should at all times be available to support those whose task it is to process applications (Authorizing Officers [AO]) and thus to provide assistance in dealing with any suspicious application. AFS personnel should regularly provide training to AOs to increase their awareness of potential fraud risks.

The MRTD-issuing authority should establish close liaisons with the issuers of breeder documents such as birth and marriage certificates and driving licences. Access to a database of death certificates assists in the prevention of fraud where an application for an MRTD is made in the name of a deceased person. The State should ensure that the departments holding records of births, marriages and deaths are reconciled and the data stored in a database, secure access to which should be available to the MRTD-issuing office. The aim is to facilitate rapid verification that submitted breeder documents are genuine and that an application is not being made, for example, in the name of a deceased person. An applicant for an MRTD who has not held one previously should be required to present himself at an MRTD-issuing office with supporting breeder documentation for an interview with an AO and, where necessary, an AFS.

An interview may also be used to process applications for an MRTD to replace an expiring one. Alternatively, provided the MRTD-issuing office has an adequate database of personal information, including portraits, a replacement application may be processed by submission of the documentation, including a new portrait, by mail. In such cases it is desirable that the

application and new portrait be endorsed by a responsible person. The return of the expiring MRTD with the new application should be required.

The MRTD-issuing office should initiate procedures that would prevent the fraudulent issue of more than one MRTD to an individual who may have attempted to assume more than one identity. Computer database checks of stored portraits using facial recognition and, where available, fingerprints can assist in this process.

Procedures in the MRTD-issuing office should prevent an applicant from selecting the AO who will serve him. Conversely the work flow should be such as to prevent any employee from selecting which applications he is to process.

The issuance of an MRTD to a young child should require the attendance at the issuing office of, preferably, both parents and of the child. This is to lower the risk of child smuggling or abduction of a child by one parent.

The replacement of an MRTD claimed to be lost or stolen should be made only after exhaustive checks including a personal interview with the applicant.

It is recommended that details, particularly document numbers, of lost or stolen MRTDs be provided to the database operated by INTERPOL. This database is available to all participating countries and can be used in the development of watch lists.

D.5 CONTROL OF ISSUING FACILITIES

A State should consider issuing all MRTDs from one or, at most, two centres. This reduces the number of places where blank documents and other secure components are stored. The control of such a central facility can be much tighter than is possible at each of many issuing centres. If central issuance is adopted, the provision of centres where applicants can attend interviews is required. Furthermore, since standard MRTDs cannot be issued instantly, a system should be established for the issue of emergency MRTDs.

— — — — — — — —

APPENDIX E TO PART 2 — ASF/SLTD KEY CONSIDERATIONS (INFORMATIVE)

Legislative requirements	Before States can begin uploading information to the INTERPOL ASF/SLTD, they must explore their legislation to determine whether they have the authority/mandate to provide international access to elements of citizens' travel document information. Should amendments to legislation be required, States should ensure that adequate coverage is provided for: 1. collection and storage of data; 2. privacy provisions (including security); 3. authorization for disseminating data to the international community; and 4. data life cycle and non-repudiation.
Data elements	A standard data set focusing on the document details rather than the holder of the document has been developed for the interchange of information pertaining to lost, stolen and revoked travel documents. States must meet the following required data fields when uploading to this database: 1. travel document identification number*; 2. type of document (passport or other); 3. issuing State's ICAO Code; 4. status of the document (i.e. stolen blank); and 5. country of theft (only mandatory for stolen blank travel documents). *Where the travel document has been personalized this should be the number contained in the MRZ; if dealing with a blank book, this number should be the serial number, if the numbers are not the same.
Information gathering	States should ensure that tools used to collect information about lost and stolen travel documents (i.e. telephone interviews, online forms) are comprehensive and conducive to securely gathering all the information required to complete the ASF/SLTD report.
Timely and accurate data provision	The strength of INTERPOL's ASF/SLTD rests on timely and accurate information. Accordingly, States should ensure that they have the systems and processes in place to share information in the most timely fashion to intercept attempts to use lost, stolen or revoked travel documents at border control. States should strive to share this information on a daily basis. Generally, once information is received that the travel document is no longer in the possession of the rightful holder or has been revoked, the issuing authority should officially record the information in its national database (if it runs and maintains one) and in the ASF/SLTD. States should also make ongoing efforts to ensure that data is accurate and reliable.

	Care must be taken to avoid input errors and to provide all the required document data, as accurate reporting is the responsibility of the issuing authority. Errors in reporting can be disruptive to travel and costly to both the traveller and issuing State. States must therefore take the necessary steps to ensure the accurate recording and reporting of lost, stolen and revoked travel documents. States should operate a round-the-clock response facility to promptly action requests for further information from INTERPOL on behalf of inquiring States.
Leveraging national databases on lost, stolen and revoked travel documents	States maintaining national databases on lost, stolen and revoked travel documents should consider using automated ways to transmit this information to INTERPOL to leverage their efforts.

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 20YY

Part 3: Specifications Common to all MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 3 — *Specifications Common to all MRTDs*
ISBN 978-92-9249-792-7

DOCUMENT CHANGE RECORD

Doc 9303, Part 3

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

Page

1. SCOPE

Part 3 defines specifications that are common to TD1, TD2 and TD3 size machine readable travel documents (MRTDs) including those necessary for global interoperability using visual inspection and machine readable (optical character recognition) means. Detailed specifications applicable to each form factor appear in Doc 9303, Parts 4 through 7.

Part 3 shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*;

and the relevant form factor specific part:

- Part 4 — *Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs*;
- Part 5 — *Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)*;
- Part 6 — *Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)*; and
- Part 7— *Machine Readable Visas*.

These specifications also apply to machine readable travel documents that contain a contactless IC i.e. electronic machine readable travel documents (eMRTDs). Specifications solely for eMRTDs are contained in the following parts of Doc 9303:

- Part 9 — *Deployment of Biometric Identification and Electronic Storage of Data in MRTDs*;
- Part 10 — *Logical Data Structure (LDS) for Storage of Biometrics and other Data in the Contactless Integrated Circuit (IC)*;
- Part 11 — *Security Mechanisms for MRTDs*; and
- Part 12 — *Public Key Infrastructure for MRTDs*.

2. PHYSICAL CHARACTERISTICS OF MRTDs

Issuing States and organizations may choose the materials to be used in the production of their travel documents. Nevertheless, no materials shall adversely affect any other component in the MRTD, and the MRTD shall, in normal use throughout its period of validity, meet the following requirements:

- *Deformation.* The MRTD shall be of a material that bends (not creases), i.e., deformation due to normal use can be flattened by the reading device without impairing the use of the MRTD or the functioning of the reader;

- *Toxicity.* The MRTD shall present no toxic hazards in the course of normal use, as specified in [ISO/IEC 7810];

- *Resistance to chemicals.* The MRTD shall be resistant to chemical effects arising from normal handling and use, except where chemical sensitivity is added for security reasons;

- *Temperature stability.* The MRTD shall remain machine readable at operating temperatures ranging from –10°C to +50°C (14°F to 122°F). The MRTD should not lose its functionality after being exposed to temperatures ranging from –35°C to +80°C (–31°F to 176°F);

- *Humidity.* The MRTD shall be machine readable at a relative air humidity ranging from 5 per cent to 95 per cent, with a maximum wet bulb temperature of 25°C (77°F), as specified in [ISO/IEC 7810]. The MRTD should not lose its reliability after being stored at, or exposed to, a relative air humidity ranging from 0 per cent to 100 per cent (non-condensing);

- *Light.* The MRTD shall resist deterioration from exposure to light encountered during normal use, as specified in [ISO/IEC 7810].

3. VISUAL INSPECTION ZONE (VIZ)

The Visual Inspection Zone of an MRTD comprises the mandatory and optional data elements designed for visual inspection. The optional data elements, together with the mandatory data elements, accommodate the diverse requirements of issuing States and organizations while maintaining sufficient uniformity to ensure global interoperability for all MRTDs.

3.1 Languages and Characters

Latin-alphabet characters, i.e. A to Z and a to z, and Arabic numerals, i.e. 1234567890 shall be used to represent data in the VIZ. Diacritics are permitted. Latin-based national characters listed in Section 6.A “Transliteration of Multinational Latin-based Characters”, e.g. Þ and ß, may also be used in the VIZ without transliteration. When mandatory data elements are in a language that does not use the Latin alphabet, a transcription or transliteration shall also be provided.

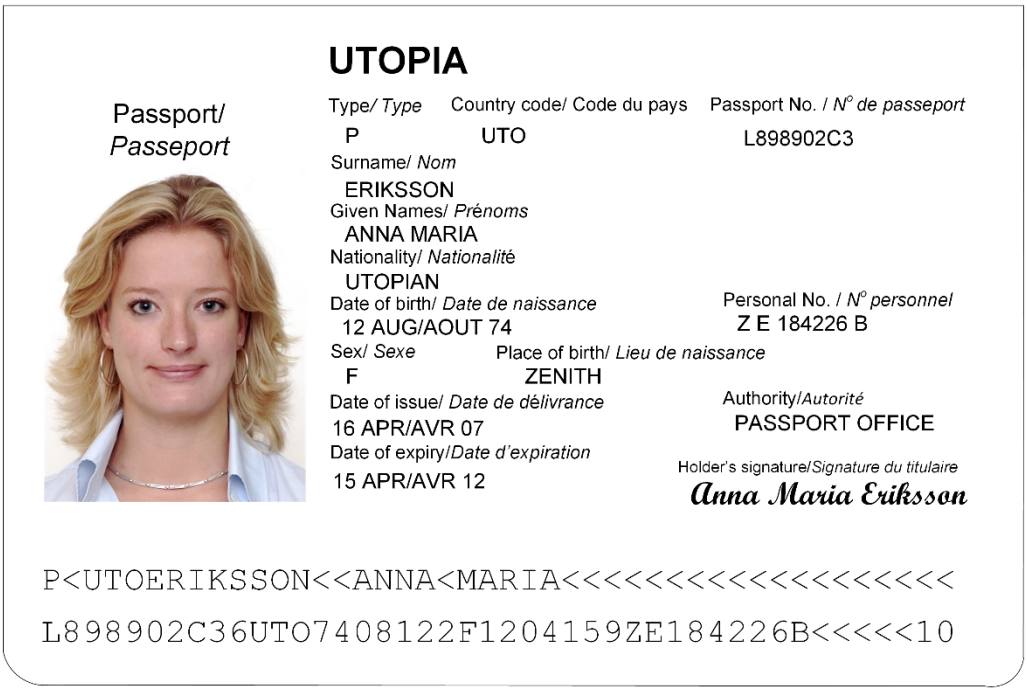


Figure 1. Example of a VIZ and MRZ from an MRTD

States that use other than Arabic numerals to represent numerical data in the VIZ shall provide a translation into Arabic numerals.

In the interests of facilitation, optional data elements should be entered in both the national language/working language of the issuing organization and either English, French or Spanish. Optional data in Zone VI may be entered entirely in the national script and/or language.

When including a translation, the different language shall be separated by an oblique character.

Punctuation may be included in the VIZ. For details see Doc 9303-4.

3.2 Typeface and Type Size

The horizontal printing density, the typeface, the type size, the font and the vertical line spacing in the VIZ are at the discretion of the issuing State or organization. For good legibility a type size with 10 characters per 25.4 mm (1.0 in) is recommended. A maximum of 15 characters per 25.4 mm (1.0 in) should not be exceeded. This type size has been chosen as the smallest in which information is clear and legible to a person with normal eyesight.

Use of upper-case characters is recommended. However, where a name includes a prefix, an appropriate mixture of upper and lower case characters may be used in the prefix (see 3.4 in this section).

Diacritical marks (accents) may be used with either lower- or upper-case characters at the option of the issuing State or organization.

3.3 Captions/Fields

Captions shall be used to identify all fields for mandatory data elements in the VIZ except as specified in the data element directories for each form factor in Doc 9303, Parts 4 to 7.

Captions may be in the official language of the issuing State or working language of the issuing organization. When such language uses the Latin alphabet, straight font style should be used to print the captions.

Where the official language of the issuing State or working language of the issuing organization is not English, French or Spanish, the printed caption shall be followed by an oblique character (/) and the equivalent of the caption in English, French or Spanish. An italic font style should be used for the second language.

Where the official language of the issuing State or working language of the issuing organization is English, French or Spanish, the issuing State or organization should use one of the other two languages to print the caption following the oblique (/) character. An italic font style should be used for the second language.

Captions shall be printed in a clear, linear type font in a size of 1.0 mm to 1.8 mm (0.04 in to 0.07 in).

When an optional field is not used, the caption shall not appear on the travel document.

3.4 Convention for Writing the Name of the Holder

The name of the holder is generally represented in two parts; the primary identifier and the secondary identifier.

The issuing State or organization shall establish which part of the name is the primary identifier. This may be the family name, the maiden name or the married name, the main name, the surname, and in some cases, the entire name where the holder's name cannot be divided into two parts. This shall be entered in the field for the primary identifier in the VIZ. It is recommended that upper-case characters be used, except in the case of a prefix, e.g. "von," "Mc" or "de la," in which case a mixture of upper and lower case is appropriate.

The remaining parts of the name are the secondary identifier. These may be the forenames, familiar names, given names, initials, or any other secondary names. These names shall be written in the field for the secondary identifier in the VIZ. It is recommended that upper-case characters be used throughout.

If a single field is used for the name, then the secondary identifier shall be separated from the primary identifier by a single comma (,). A comma is not needed if multiple fields are used.

Prefixes and suffixes including titles, professional and academic qualifications, honours, awards, and hereditary status, should not be included in the VIZ. However, if an issuing State or organization considers such a prefix or suffix to be legally part of the name, the prefix or suffix can appear in the VIZ. Numeric characters should not be written in the name fields of the VIZ; however, where the use of numeric characters is a legal naming convention in the issuing State, these should be represented in Roman numerals. Any prefixes, suffixes or Roman numerals shall be entered in the secondary identifier field.

National characters may be used in the VIZ. If the national characters are not Latin-based, a transcription or transliteration into Latin characters shall be provided.

3.5 Representation of Issuing State or Organization

Where the name of the issuing State or organization and/or the location of the issuing office or authority are in a language

that does not use Latin characters, the name of the State or other location shall appear in the national language/working language of the issuing organization and also shall be either:

- transliterated into Latin characters; or
- translated into one or more languages (at least one of which must be English, French or Spanish) by which the name may be more commonly known to the international community.

The name in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

Where the name of the issuing State or organization or location of the issuing office or authority is in a language that uses the Latin alphabet, but the name is more familiar to the international community in its translation into another language or languages (particularly English, French or Spanish), the name should be accompanied by one or more translations. The name in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

3.6 Representation of Nationality

The nationality of the holder in the VIZ, in documents where this field is mandatory, shall be represented either by the three-letter code (see Section 5) or in full at the discretion of the issuing State or organization.

If the nationality is written in full and the national language of the issuing State or working language of the issuing organization is a language that does not use Latin characters, the nationality shall appear in the national/working language and also shall be either:

- transliterated into Latin characters; or
- translated into one or more languages (at least one of which must be English, French or Spanish) by which the nationality may be more commonly known to the international community.

The nationality in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

Where the national language of the issuing State or working language of the issuing organization uses the Latin alphabet, but the nationality is more familiar to the international community in its translation into another language or languages (particularly English, French or Spanish), the nationality in the national/working language should be accompanied by one or more translations. The nationality in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

3.7 Representation of Place of Birth

Inclusion of the place of birth is optional. If the place of birth is included it may be represented by the town, the city, the suburb and/or the state.

If the town, city or suburb is included and the national language of the issuing State or working language of the issuing authority is a language that does not use Latin characters, the town, city or suburb shall appear in the national/working language and also shall be either:

- transliterated into Latin characters; or
- translated into one or more languages (at least one of which must be English, French or Spanish) by

which it may be more commonly known to the international community.

The town, city or suburb in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

Where the national language of the issuing State or working language of the issuing organization uses the Latin alphabet, but the town, city or suburb is more familiar to the international community in its translation into another language or languages (particularly English, French or Spanish), the town, city or suburb in the national/working language should be accompanied by one or more translations. The town, city or suburb in the different languages shall be separated by an oblique character (/) followed by at least one blank space.

If the State is included it's three-letter code shall be represented as outlined in Section 5, except where no code for the State of Birth exists, in which case the name shall be written in full, and the requirements for translation and transliteration identified for town, city and suburb above apply.

Note.— When choosing to include or omit the Place of Birth, the travel document issuing State or organization should take into consideration any current political sensitivities linked to the State or territory and whether it is a State or territory recognized by visa-issuing authorities in other countries.

3.8 Representation of Dates

Dates in the VIZ of the MRTD shall be entered in accordance with the Gregorian calendar as follows:

Day

Days shall be shown by a two-digit number, i.e. the dates from one to nine shall be preceded by a zero. This number may be followed by a blank space before the month or may be followed immediately by the month, with no blank space.

Month

The month may be printed in full in the national language of the issuing State or working language of the issuing organization or abbreviated, using up to four character positions.

Where the national language of the issuing State or working language of the issuing organization is not English, French or Spanish, the month shall be followed by an oblique character (/) and the month or the abbreviation of the month up to four character positions, in one of the three languages, as shown in the table below.

Where the national language of the issuing State or working language of the issuing organization is English, French or Spanish, the issuing State or organization may also use one of the other two languages (shown in Table 1) following the oblique character (/).

The month may alternatively be printed in numerical form at the discretion of the issuing State or organization, particularly where this might facilitate the use of the MRTD by States using other than the Gregorian calendar. In this case the date would be written DDnMMnYY or DDnMMnYYYY, where n = a single blank space or a period.

Table 1. Abbreviations of Months in English, French and Spanish

Month	*English*	*French*	*Spanish*
JANUARY	JAN	JAN	ENE
FEBRUARY	FEB	FÉV	FEB
MARCH	MAR	MARS	MAR
APRIL	APR	AVR	ABR
MAY	MAY	MAI	MAYO
JUNE	JUN	JUIN	JUN
JULY	JUL	JUIL	JUL
AUGUST	AUG	AOÛT	AGO
SEPTEMBER	SEP	SEPT	SEPT
OCTOBER	OCT	OCT	OCT
NOVEMBER	NOV	NOV	NOV
DECEMBER	DEC	DÉC	DIC

Year

The year will be shown by the last two or four digits and may be preceded by a blank space, or it may follow the month immediately with no blank space. Both formats are acceptable.

When the month is represented numerically, the issuing State or organization may use the two- or four-digit representation of the year, and separate the month and year by a blank space or a period.

Note.— States are encouraged to use the four digit representation of the year for all date formats.

Examples:

12 July 1942 on an MRTD data page issued in Italian with French translation of the month could appear as:

12nLUGn/JUILn1942

where n = a single blank space, i.e. 12 LUG /JUIL 1942

or

12nLUGn/JUILn42

where n = a single blank space, i.e. 12 LUG /JUIL 42

or

12 July 1942 or 12 July 42 (using English only)

or

12JUIL1942 or 12JUIL42 (using French abbreviation)

or

12JUL 1942 or 12JUL 42 (using English or Spanish abbreviation)

or

12 07 42 or 12.07.42 (using numerical format).

or

12 07 1942 or 12.07.1942 (using numerical format with four-digit year).

Unknown date of birth. Where a date of birth is completely unknown, that data element shall appear in the date format used for dates of birth by the issuing State or organization but with Xs representing unknown elements (numbers and/or letters) of the date.

Examples:
XXnXXnXX
XXnXXnXXXX
XXnXXXnXX where n = a single blank space or a period (if numerical format is used).

If only part of the date of birth is unknown, only that part (day, month, year) of the date shall be represented by Xs as per the date format used by the issuing State or organization.

3.9 Displayed Identification Features of the Holder

Doc 9303 identifies mandatory and optional identification feature(s) of the holder which must be displayed within the VIZ, i.e. facial image, signature or usual mark and/or single-digit fingerprint for each type of MRTD as well as the position, dimensions and scaling for the identification features.

3.9.1 Displayed facial image

To ensure compatibility with facial recognition systems, portrait capturing shall comply with relevant specifications outlined in [ISO/IEC 39794-5].

The displayed facial image, whether provided in paper or digital format, shall:

- be digitally printed in the MRTD;
- depict a true likeness of the rightful holder of the MRTD; and
- not be digitally altered or enhanced to change the subject's appearance in any way.

Necessary measures shall be taken by the issuing State or organization to ensure that the displayed portrait is resistant to forgery and substitution.

3.9.1.1 Image Printing for Portrait Submission

The physical portrait shall yield an accurate recognizable representation of the subject. The quality of the original captured image should at least be comparable to the minimum quality acceptable for paper photographs (resolution comparable to 6 – 8 line pairs per millimetre). To achieve this comparable image quality in a digital reproduction, careful attention shall be given to the image capture, processing, digitization, compression and printing technology and the process used to produce the portrait. The printing process shall maintain the width to height ratio of the original image.

Note.—*Many issuing states use a printing/re-scanning procedure for document application. This approach is acceptable; however, caution should be taken to ensure quality according to the guidelines and requirements indicated below and in [ISO/IEC 39794-5]. If a new design of the application process is considered, digital submission should be taken into consideration as the preferred technology whenever possible.*

Print resolution. The printing process should produce a smooth image that is capable of accurately rendering fine contrasted facial details, such as wrinkles and moles. All flesh tones from both light- and dark-complexioned subjects should be printed accurately and limited hot spots or shadow drop-outs apparent. Smooth facial details should be rendered without noticeable posterization or contouring.

Saturation and colour. With the exception of glare or glints caused by small areas of possible specular (mirror-like) reflection, only a small portion of the printed image should be saturated in white or black. Excluding the background area, using luminosity, the number of fully saturated 0 value pixels shall be less than 0.1%, and the number of fully saturated 255 value pixels shall be less than 0.1%.

No portion of the background or the subject's garments should be printed fully white and details should be apparent in dark shadow regions.

Printed photos shall be colour images having balanced colour channels. It may be assumed that the capture device (digital camera or scanner) is correctly white balanced.

Paper properties and portrait size. The photograph shall be on photo-quality paper. Examples of such paper are the following (other technologies with similar properties are also acceptable):

- Instant photographic standard gloss,
- Dye sublimation photographic semi-gloss,
- Silver halide photographic semi-gloss, or
- Drylab photographic inkjet bases standard gloss.

The photograph paper shall have a low roughness, non-structured surface (no pearl or silkscreen effect). Submitted portraits should have a minimum width of 35 mm. The inter eye distance (IED) should be at least 10 mm.

Newly designed application processes still relying on printed portrait submission should consider using larger photo sizes, such as, e.g., 7 cm by 10 cm. Larger photos reduce the risk of quality losses in the process chain. However, a switch to larger photos will have process implications to be considered.

Moiré or visible dot patterns. Digitization of printed photos may introduce artefacts, such as moiré, and certain printing processes may exacerbate the generation of such artefacts. The printing process employed should allow accurate face recognition when its prints are scanned with a document scanner at a spatial sampling rate of 120 pixels per centimetre (300 pixels per inch) in each axis.

If a printed photo has been produced through a periodic half-toning process, scanning the photo will almost invariably introduce moiré patterns. Thus, those printers, such as inkjet and laser printers, which inherently employ half-toning to simulate continuous tones, should use non-periodic (or dithered) half-toning methods. Furthermore, the printing process should not produce dot patterns visible to the unaided eye.

Note.— *It is often useful to provide a transparent template to a person responsible for photo quality evaluation. The template would display the limits of head size and rotation (roll) and, when superimposed on the photo, could assist in the determination of whether a printed photo is compliant to the requirements. Samples of such tools can be found in [ISO/IEC 39794-5].*

3.9.1.2 Scanning of Submitted Portraits

Submitted portraits shall comply with the relevant specifications outlined in section 3.9.1.1 and in [ISO/IEC 39794-5].

Properties of the submitted portrait. Submitted portraits should be 45.0 mm x 35.0 mm (1.77 in x 1.38 in) in dimension. This will provide adequate resolution for scaling to required size for use on the MRTD while having adequate resolution for facial recognition purposes.

Multiple scan/print steps shall not be used in an application process. If the portrait has been printed for submission and is subsequently scanned, all remaining production steps shall be digital.

A submitted portrait shall have been captured within the last six months before application, as outlined in [ISO/IEC 39794-5]. Portraits with a capture time dating back more than three months should not be accepted. Issuers should consider the use of the metadata encoded with the digital image to assure that the photograph is recent.

If printed portraits are submitted, evidence on the capturing date should be requested. This may be the printed manufacturing date on the back side of the photo, or a dated invoice of the photographer. The complete card should be provided if the portrait is part of a photo card (e.g., a 10x15 print containing 2x2 images).

The submitted portrait shall be clean, not bent, not scratched, not folded and not damaged. There shall be no ink marks or creases on the printed portrait.

Where the portrait is supplied to the issuing authority in digital form, the requirements specified by the issuing authority must be adhered to.

Pixel count and Modulation Transform Function (MTF). The finally scanned images shall have a pixel count as specified in [ISO/IEC 39794-5]. MTF20 should occur at 4,7 cy/mm or higher for scanners. The scanner's MTF should be the same in both axes. Image enhancement processing using either built-in hardware or software-based image sharpening generally should not be used to boost the MTF.

Example:

The optical properties of the image can be maintained if the digital camera original image MTF20 should occur at approximately 80% or higher of the Nyquist frequency when using the MTF test method according to [ISO 12233]. The size of a freckle/mole that should be detectable in face photos is 2 to 3 mm. Rulers make good fiducial markers to make measurements on the image.

The MTF analysis should be done using the appropriate target from ISO 12233. Informative examples can be found in [ISO/IEC 39794-5].

Example:

A typical printed image with 10 mm IED should be scanned at a sampling rate of at least 300 ppi.

The MTF will be limited by the size of the paper photo and the resolution (fineness of detail) therein. To obtain higher resolution from scanned images the issuer should consider increasing the size requirement for printed portraits.

Particular care shall be taken in the acquisition process in order to avoid any kind of image dimensional stretching in any direction.

The width to height ratio of the final image is defined by the application process of the issuer, a typical value is 7:9. Necessary modifications shall be made by cropping and shall not be made by stretching.

Colour, sharpness, and saturation. The scanned portrait shall have the same colour as the submitted one. The human eye shall not be able to detect differences between the portrait and scanned result when viewed on a colour corrected display device and under daylight conditions. The portrait shall have appropriate brightness and contrast that show skin tones naturally.

The number of quantization levels should be at least 256 levels per colour, with three colours per pixel. The scanned image shall comply with the colour requirements outlined in [ISO/IEC 39794-5].

Since red-green-blue (RGB) colour space and its derivatives are inherently device-dependent, the scanner's output shall be converted to one of the well-defined, device-independent colour spaces as outlined in [ISO/IEC 39794-5].

Saturation occurs when significant numbers of pixels have values that are at the limits of quantization, i.e., at the levels of 0 or 255, if quantization of eight bits per colour is employed. Acceptable scanned face images should not have a significant number of pixels in saturation in the facial region.

The scanned portrait shall be centred, clear and in sharp focus with no shadows. It shall not have visible compression artefacts.

3.9.1.3 Image Printing for MRTD production

The portrait printed on the data page shall be derived from the same digital image source as the image stored electronically in the MRTD. However, due to the influence of printing technologies as well as to the application of several security features to the portrait and to the data page, the image may not be exactly the same. Examples for possible deviations are the printer resolution, removed background in the printed portrait, image enhancements, dithering of grayscale content, or guilloches occurring in the print.

Note.—*The implementation of the portrait on or into the MRTD should be done considering the properties of the different materials and technologies in use. It is possible that the printing technology itself introduces specific features into the printed portrait.*

The digital reproduction shall yield an accurate recognizable representation of the subject. To achieve such image quality in a document data page, careful attention shall be given to the processing, compression and printing technology and the process used to produce the portrait. Printed portraits have specific features which depend on categories of printing technologies.

The primary printed image on the MRTD may be either greyscale or colour.

Any face printing process should produce a smooth image that is capable of accurately rendering fine facial details, such

as contrasted wrinkles, contrasted moles, and contrasted scars, as small as two millimeters in diameter on the face positioned anywhere in the printed image area. Such details shall be detectable when viewed with the naked eye at a distance of 0.3 m.

All flesh tones from both light- and dark-complexioned subjects should be printed accurately and no hot spots or shadow drop-out should be apparent. Smooth facial details should be rendered without posterization or contouring.

Size. The portrait dimensions should meet the specifications outlined in [ISO/IEC 39794-5]. Necessary modifications shall be made by cropping and shall not be made by stretching. In cases where the background has been removed from the image, the correct width or height of the printed image may be impossible to determine. In such cases the height-to-width ratio is considered to be maintained if the ratio between *IED* and eye to mouth distance (*EM)* of the printed image is the same as of the portrait.

Tonal range. The tonal range of the printed image shall not interfere with facial details important for human identification when making a comparison of the printed image to the document holder.

Moiré or visible dot patterns. Moiré or dot patterns in the printed image should be minimized. Any such patterns in the printed image shall not interfere with facial details important for human identification when making a comparison of the printed image to the document holder.

Portrait placement in an MRTD and coexistence with security printing. The printed portrait shall be centred within Zone V, with the crown (top of the head ignoring any hair) nearest the top edge of the MRTD. The crown-to-chin portion of the facial image shall be 70 to 80 per cent of the longest dimension defined for Zone V, maintaining the aspect ratio between the crown-to-chin and ear-to-ear details of the face of the holder. The 70 to 80 per cent requirement may mean cropping the picture so that not all the hair is visible.

If present, a digitally printed reproduction shall coexist with background security treatment(s) located within Zone V, i.e., the background security printing shall not interfere with proper viewing of the displayed portrait, and vice versa, yet still offer protection to the displayed portrait.

Coexistence with final preparation treatment(s) of the MRTD. A displayed portrait shall coexist with final preparation treatment(s), i.e. final preparation treatment(s) shall not interfere with proper viewing of the displayed portrait, and vice versa.

Border. A border or frame shall not be used to outline a digitally printed reproduction.

3.9.1.6 Compliance with international standards

The photograph shall comply with the appropriate definitions set out in [ISO/IEC 39794-5].

3.9.2 Displayed signature or usual mark

A displayed signature or usual mark, the acceptability of which is at the issuing State or organization’s discretion, appears in Zone IV. A displayed signature or usual mark shall be an original created on the MRTD, a digitally printed reproduction of an original or, where permitted by specifications defined in Doc 9303 Parts 4 to 7 specific to the preparation of the different types of MRTDs, on a substrate that can be securely affixed to the MRTD. Necessary measures shall be taken by the issuing State or organization to ensure that the displayed signature or usual mark is resistant to forgery and substitution. The displayed signature or usual mark shall meet the following requirements.

Orientation. The displayed signature or usual mark shall be displayed with its A-dimension parallel to the reference (longer) edge of the MRTD as defined in Figure 2.

Size. The displayed signature or usual mark shall be of such dimensions that it is discernible by the human eye (i.e. reduced in size by no more than 50 per cent), and the aspect ratio (A-dimension to B-dimension) of the original signature or usual mark is maintained.

Scaling for reproduction using digital printing. In the event the displayed signature or usual mark is scaled up or scaled down, the aspect ratio (A-dimension to B-dimension) of the original signature or usual mark shall be maintained.

Cropping for reproduction using digital printing. The issuing State or organization should take steps to eliminate or minimize cropping.

Colour. The displayed signature or usual mark shall be displayed in a colour that affords a definite contrast to the background.

Borders. Borders or frames shall not be permitted or used to outline the displayed signature or usual mark.

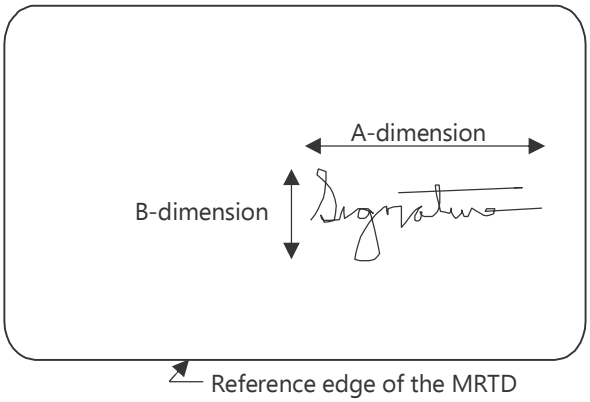


Figure 2. Orientation of the displayed signature or usual mark

3.9.3 Displayed single-digit fingerprint

A displayed single-digit fingerprint, if required by the issuing State or organization, shall be either an original created on the MRTD substrate by the holder or, more probably, a digitally printed reproduction of an original. Necessary measures shall be taken by the issuing State or organization to ensure that the single-digit fingerprint is resistant to forgery and substitution. The single-digit fingerprint shall meet the following requirements.

Orientation. The A-dimension (width) of the displayed single-digit fingerprint shall be parallel to the reference edge of the MRTD as defined in Figure 3. The top of the finger shall be that portion of the single-digit fingerprint furthest away from the reference edge of the MRTD. (See Doc 9303-6, Figure 10 and Figure 12.)

Size. The displayed single-digit fingerprint shall be a one-to-one replication (A-dimension versus B-dimension) of the original print.

Scaling for reproduction using digital printing. Scaling of a single-digit fingerprint shall not be permitted.

Cropping for reproduction using digital printing. The issuing State or organization should take steps to eliminate or minimize cropping.

Colour. The displayed single-digit fingerprint shall be displayed in a colour that affords a definite contrast to the background.

Borders. Borders or frames shall not be permitted or used to outline the displayed single-digit fingerprint.

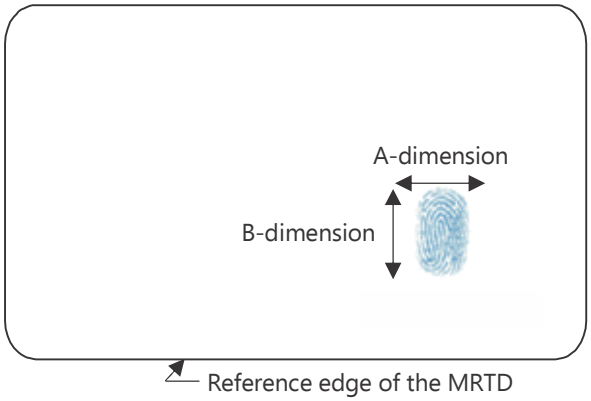


Figure 3. Orientation of the displayed single-digit fingerprint

4. MACHINE READABLE ZONE (MRZ)

4.1 Purpose of the MRZ

MRTDs produced in accordance with Doc 9303 incorporate an MRZ to facilitate inspection of travel documents and reduce the time taken up in the travel process by administrative procedures. In addition, the MRZ provides verification of the information in the VIZ and may be used to provide search characters for a database inquiry. As well, it may be used to capture data for registration of arrival and departure or simply to point to an existing record in a database.

The MRZ provides a set of essential data elements in a format, standardized for each type of MRTD that can be used by all receiving States regardless of their national script or customs.

The data in the MRZ are formatted in such a way as to be readable by machines with standard capability worldwide. It must be stressed that the MRZ is reserved for data intended for international use in conformance with international standards for MRTDs. The MRZ is a different representation of the data than is found in the VIZ.

4.2 Properties of the MRZ

The data in the MRZ must be visually readable as well as machine readable. Data presentation must conform to a common standard such that all machine readers configured in conformance with Doc 9303 can recognize each character and communicate in a standard protocol (e.g. ASCII) that is compatible with the technology infrastructure and the processing requirements defined by the receiving State.

To meet these requirements, OCR-B typeface is the specified medium for storage of data in the MRZ. The MRZ as defined herein is recognized as the machine reading technology essential for global interchange and is therefore mandatory in all types of MRTDs.

4.3 Constraints of the MRZ

The only characters allowed in the MRZ are a common set of characters (Figure 4) which can be used by all States. National characters generally appear only in the computer-processing systems of the States in which they apply and are not available globally. They shall not, therefore, appear in the MRZ.

Diacritical marks are not permitted in the MRZ. Even though they may be useful to distinguish names, the use of diacritical marks in the MRZ would confuse machine-reading equipment, resulting in less accurate database searches and slower clearance of travellers.

The number of character positions available for data in the MRZ is limited and varies according to the type of MRTD. The length of the data elements inserted in the MRZ must conform to the size of the respective fields as specified in the MRZ data element directory in the applicable Part 4 to 7 of Doc 9303.

In some instances, names in the MRZ may not appear in the same form as in the VIZ. In the VIZ, non-Latin and national characters may be used to represent more accurately the data in the script of the issuing State or organization. Such characters are not permitted in the MRZ.

4.4 Print Specifications

Machine readable data shall be printed in OCR-B type font, size 1, constant stroke width characters, at a fixed width spacing of 2.54 mm (0.1 in), i.e. horizontal printing density of 10 characters per 25.4 mm (1.0 in). Printed characters are restricted to those defined in Figure 4.

Figure 4. Subset of OCR-B Characters from [ISO 1073-2] for use in machine readable travel documents

Note.— For illustrative purposes only – the characters shown are larger than actual size.

4.5 Machine Reading Requirements and the Effective Reading Zone

Effective reading zone. A fixed-dimensional reading area (effective reading zone (ERZ) of 17.0 mm × 118.0 mm (0.67 in × 4.65 in)), sized to accommodate the largest MRTD, is defined to allow use of a single machine reader for all sizes of MRTDs. The location of the ERZ is as defined in Figure 5. The provision of the ERZ is not intended to allow additional tolerance for the printing positions defined in Parts 4, 5, 6 and 7 specific to the preparation of the different types of MRTDs. The ERZ is intended to allow for variances due to the manual placement of machine readable visas (MRVs) and the fanning effect of the pages that takes place when reading an interior page of an MRP. It also allows for the reading of MRTDs with either two or three lines of machine readable data.

To combat the threat to travel document security posed by, for example, photocopiers, security features are permitted in the MRZ, and any such security feature shall not interfere with accurate reading of the OCR characters at the B900 range, as defined in [ISO 1831]. While OCR characters must be visible, as specified in 4.2, to ensure that all MRTDs, including those with security features in the MRZ, can be successfully read, the OCR characters in the MRZ shall be machine readable at least in the near infrared portion of the spectrum (i.e. the B900 band defined in [ISO 1831]).

Note.— The dimensions of the effective reading zone (ERZ) illustrated are based on a standardized ERZ for all machine readable travel documents to allow use of a single machine reader.

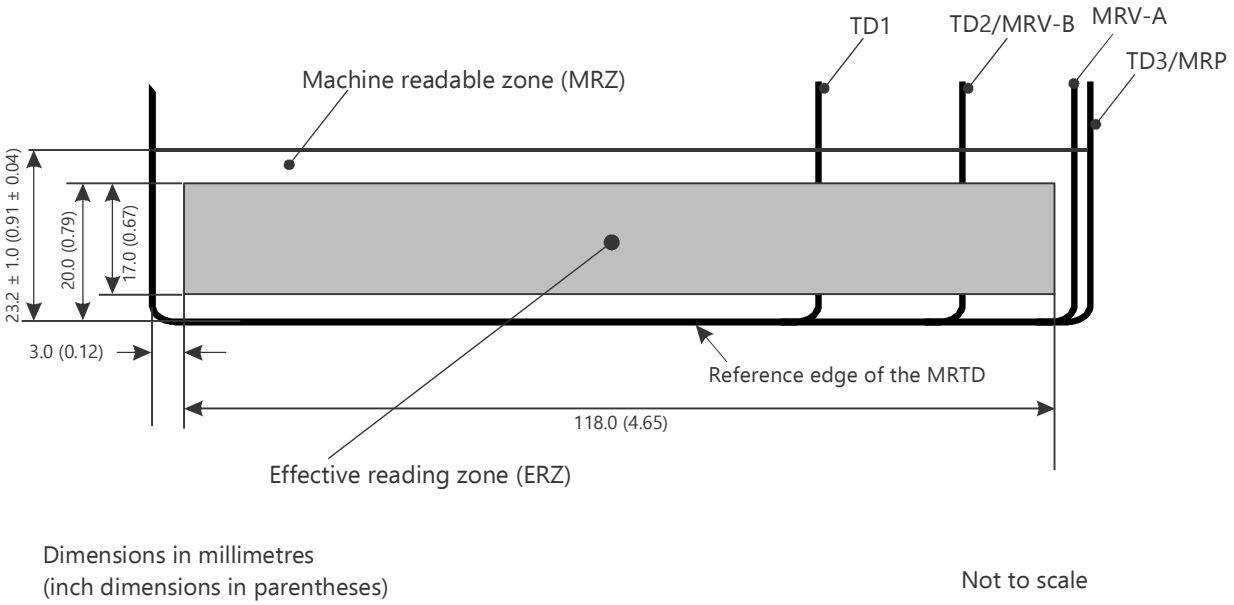


Figure 5. Schematic diagram of the MRTD effective reading zone

4.6 Convention for Writing the Name of the Holder

To achieve global interoperability, the primary and secondary identifiers in the MRZ shall be printed using upper-case OCR-B characters, illustrated in Figure 4, without diacritical marks, and conform to the number of character positions available. As such, names in the MRZ are represented differently from those in the VIZ. The issuing State or organization shall transliterate national characters using only the allowed OCR-B characters and/or truncate, as specified in the form factor specific Parts 4 to 7 of Doc 9303. Transliteration tables for the most commonly used Latin, Cyrillic and Arabic families of languages are provided in Section 6.

The primary identifier, using the Latin character transliteration (if applicable), shall be written in the MRZ as specified in the form factor specific Parts 4 to 7 of Doc 9303. The primary identifier shall be followed by two filler characters (<<). The secondary identifier, using the Latin character transliteration (if applicable), shall be written starting in the character position immediately following the two filler characters.

If the primary or secondary identifiers have more than one name component, each component shall be separated by a single filler character (<).

Filler characters (<) should be inserted immediately following the final secondary identifier (or following the primary identifier in the case of a name having only a primary identifier) through to the last character position in the machine readable line.

The number of character positions in the name field is limited and differs for the different types of MRTDs. If the primary and secondary identifiers, written in the relevant machine readable line using the above procedure, exceed the available character positions, then truncation shall be carried out using the procedure set out in the form factor specific Parts 4 to 7 of Doc 9303. In all other cases, the name shall not be truncated.

Examples of truncation of names are contained in the form factor specific Parts 4 to 7 of Doc 9303.

Prefixes and suffixes, including titles, professional and academic qualifications, honours, awards, and hereditary status (such as Dr., Sir, Jr., Sr., II and III) shall not be included in the MRZ except where the issuing State considers these to be legally part of the name. In such cases, prefixes or suffixes shall be represented as components of the secondary identifier(s).

Numeric characters shall not be used in the name fields of the MRZ.

Punctuation characters are not allowed in the MRZ. Where these appear as part of a name, they should be treated as follows:

Apostrophe:

This shall be omitted; name components separated by the apostrophe shall be combined, and no filler character shall be inserted in its place in the MRZ.

Example VIZ: D’ARTAGNAN
MRZ: `DARTAGNAN`

Hyphen:

Where a hyphen appears between two name components, it shall be represented in the MRZ by a single filler character (<). (i.e. hyphenated names shall be represented as separate components).

Example VIZ: MARIE-ELISE
MRZ: `MARIE<ELISE`

Comma:

Where a comma is used in the VIZ to separate the primary and secondary identifiers, the comma shall be omitted in the MRZ, and the primary and secondary identifiers shall be separated in the MRZ by two filler characters (<<).

Example VIZ: ERIKSSON, ANNA MARIA
MRZ: `ERIKSSON<<ANNA<MARIA`

Otherwise, where a comma is used in the VIZ to separate two name components, it shall be represented

in the MRZ as a single filler character (<).

Example VIZ: ANNA, MARIA
MRZ: ANNA<MARIA

Other punctuation characters:
All other punctuation characters shall be omitted from the MRZ (i.e. no filler character shall be inserted in their place in the MRZ).

4.7 Representation of Issuing State or Organization and Nationality of Holder

The three-letter codes referenced in Section 5 shall be used to complete the fields for the issuing State or organization and the nationality of the holder in the MRZ.

4.8 Representation of Dates

Dates in the MRZ of the MRTD shall be shown as a six-digit string consisting of the last two digits for the year (YY) immediately followed by two digits for the number of the month (MM) and by two digits for the day (DD). The structure is as follows: YYMMDD.

Following this format, 12 July 1942 will be shown as: 420712.

If all or part of the date of birth is unknown, the relevant character positions shall be completed with filler characters (<).

4.9 Check Digits in the MRZ

A check digit consists of a single digit computed from the other digits in a series. Check digits in the MRZ are calculated on specified numerical data elements in the MRZ. The check digits permit readers to verify that data in the MRZ is correctly interpreted.

A special check digit calculation has been adopted for use in MRTDs. The check digits shall be calculated on modulus 10 with a continuously repetitive weighting of 731 731 ..., as follows.

Step 1. Going from left to right, multiply each digit of the pertinent numerical data element by the weighting figure appearing in the corresponding sequential position.

Step 2. Add the products of each multiplication.

Step 3. Divide the sum by 10 (the modulus).

Step 4. The remainder shall be the check digit.

For data elements in which the number does not occupy all available character positions, the symbol < shall be used to complete vacant positions and shall be given the value of zero for the purpose of calculating the check digit.

When the check digit calculation is applied to data elements containing alphabetic characters, the characters A to Z shall have the values 10 to 35 consecutively, as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Data elements included in the check digit calculation and check digit location for each document type are contained in the form factor specific Parts 4 to 7 of Doc 9303. Examples of check digit calculation are found in Informative Appendix A to this Part.

4.10 Characteristics of the MRZ

Except as otherwise specified herein, the MRTD shall conform with [ISO 1831] concerning the following matters:

- optical properties of the substrate to be used;
- optical and dimensional properties of the image patterns forming OCR characters; and
- basic requirements related to the position of OCR characters on the substrate.

Machine readable data shall be arranged from left to right in fixed-length fields in two lines (upper and lower) except for TD1 size travel documents where there are three lines (upper, middle and lower). The data are presented in the order specified in the data structure tables in the form factor specific Parts 4 to 7 of Doc 9303 and located on the document as shown in those parts. Data shall be entered in each field, beginning with the left-hand character position.

Where the entered data do not occupy all the character positions specified for the relevant field, the symbol < shall be used to fill the unoccupied positions.

4.11 Quality Specifications of the MRZ

In general, the print quality shall conform to [ISO 1831] Range X, except as otherwise provided herein. Except where otherwise noted, all quality specifications set forth hereunder shall conform to the requirements of Section 2 of this Part and shall apply to the MRTD after final preparation and, in the case of visas, after placement in the passport or other travel document.

Substrate quality. [ISO 1831], 4.3 through 4.3.2, shall be used for reference only.

Substrate opacity. The substrate used, measured before and after final preparation (and for visas, prior to placement in the passport or other travel document), shall be within the definition of at least medium opacity as specified in [ISO 1831], 4.4.1 and 4.4.3.

Substrate gloss. The level of gloss is not specified.

Fluorescence. The reflectance of the substrate in the visible spectrum shall exhibit no visibly detectable fluorescence when irradiated by ultraviolet light, except where this is a predictable fluorescence for security reasons.

Alternative substrates. The aforementioned quality specifications should be followed irrespective of the substrate material.

Spectral band. The OCR print shall be legible visually and shall be black (B425 through B680 as defined in [ISO 1831]). The OCR print shall also absorb in the B900 band as defined in [ISO 1831] (i.e. near infrared). This property must test successfully when the characters are machine-read through any protective material that may have been applied to the

surface of the document.

Print contrast signal (PCS). After final preparation, the minimum print contrast signal (PCS/min), when measured as specified in [ISO 1831], shall be as follows: PCS/ min ≥ 0.6 at the B900 spectral band.

Character stroke width. The stroke width after final preparation shall be as specified for Range X in [ISO 1831], 5.3.1.

Contrast variation ratio (CVR). After final preparation, the CVR should be as is shown for Range X in [ISO 1831], i.e. CVR < 1.50.

Spots and extraneous marks. [ISO 1831], 5.4.4.6 and 5.4.5.12 shall apply at the reading surface (see also B.6 of Appendix B and C.5.10 of Appendix C to [ISO 1831]).

Voids. The value of "d" as defined in [ISO 1831], 5.4.5.9 shall be equal to 0.4 at the reading surface.

Line separation. Refer to the form factor specific Parts 4 to 7 of Doc 9303.

Line spacing. Refer to the form factor specific Parts 4 to 7 of Doc 9303.

Skew of the MRZ lines. The effect of the actual skew of the MRZ lines and the actual skew of the MRZ characters shall not exceed 3 degrees measured from the reference edge nor shall the skew of MRZ or character misalignment result in the MRZ lines or any part thereof appearing outside the printing zone as defined in the form factor specific Parts 4 to 7 of Doc 9303.

5. CODES FOR NATIONALITY, PLACE OF BIRTH, LOCATION OF ISSUING STATE/AUTHORITY AND OTHER PURPOSES

Part A — Letter Codes

Two- and three-letter codes shall be obtained from the [ISO 3166] maintenance agency - [ISO 3166/MA], ISO's focal point for country codes. These codes are regularly updated in [ISO 3166-1] and are publically available (https://www.iso.org/iso-3166-country-codes.html).

Codes not included in [ISO 3166-1], such as extensions for other States and organizations, or other exceptions, are outlined in the table that follows.

Entity (short name)	2-letter code	3-letter code	*Entity (short name)*	2-letter code	3-letter code
British Overseas Territories Citizen		GBD	British Subject		GBS
British National (Overseas)		GBN	British Protected person		GBP
British Overseas Citizen		GBO	Republic of Kosovo[1]	KS	RKS

[1] The KS and RKS codes are operationally in use, although not reflected in [ISO 3166-1].

Part B — Other Codes Reserved by ISO 3166/MA

European Union (EU)	EU	EUE

Part C — Codes for Use in United Nations Travel Documents

United Nations Organization or one of its officials	UN	UNO
United Nations specialized agency or one of its officials	UN	UNA
Resident of Kosovo to whom a travel document has been issued by the United Nations Interim Administration Mission in Kosovo (UNMIK)		UNK

Part D — Codes for Other Issuing Authorities

African Development Bank (ADB)		XBA
African Export-Import Bank (AFREXIM bank)		XIM
Caribbean Community or one of its emissaries (CARICOM)		XCC
Council of Europe		XCE
Common Market for Eastern and Southern Africa (COMESA)		XCO
Economic Community of West African States (ECOWAS)		XEC
International Criminal Police Organization (INTERPOL)		XPO
Organization of Eastern Caribbean States (OECS)		XES
Sovereign Military Order of Malta or one of its emissaries		XOM
Southern African Development Community		XDC

Part E — Codes for Persons Without a Defined Nationality

Stateless person, as defined in Article 1 of the 1954 Convention Relating to the Status of Stateless Persons		XXA
Refugee, as defined in Article 1 of the 1951 Convention Relating to the Status of Refugees as amended by the 1967 Protocol		XXB
Refugee, other than as defined under the code XXB above		XXC
Person of unspecified nationality, for whom issuing State does not consider it necessary to specify any of the codes XXA, XXB or XXC above, whatever that person's status may be. This category may include a person who is neither stateless nor a refugee but who is of unknown nationality and legally residing in the State of issue.		XXX

Part F — Codes Deprecated in [ISO 3166] (referenced for backward compatibility)

Netherlands Antilles	AN	ANT
Neutral Zone	NT	NTZ

Part G — Codes Used in Specimen Documents

In order to establish a standardized way to identify specimen documents, it is recommended to set the nationality of the document holder to "Utopia" for sample documents.

Utopia	UT	UTO

6. TRANSLITERATIONS RECOMMENDED FOR USE BY STATES

The following tables contain the most commonly used national characters of the Latin, Cyrillic and Arabic families of languages.

A. Transliteration of Multinational Latin-based Characters

Unicode	*National character*	*Description*	*Recommended transliteration*
00C0	À	A grave	A
00C1	Á	A acute	A
00C2	Â	A circumflex	A

Unicode	*National character*	*Description*	*Recommended transliteration*
00C3	Ã	A tilde	A
00C4	Ä	A diaeresis	AE or A
00C5	Å	A ring above	AA or A
00C6	Æ	ligature AE	AE
00C7	Ç	C cedilla	C
00C8	È	E grave	E
00C9	É	E acute	E
00CA	Ê	E circumflex	E
00CB	Ë	E diaeresis	E
00CC	Ì	I grave	I
00CD	Í	I acute	I
00CE	Î	I circumflex	I
00CF	Ï	I diaeresis	I
00D0	Đ	Eth	D
00D1	Ñ	N tilde	N or NXX
00D2	Ò	O grave	O
00D3	Ó	O acute	O
00D4	Ô	O circumflex	O
00D5	Õ	O tilde	O
00D6	Ö	O diaeresis	OE or O
00D8	Ø	O stroke	OE
00D9	Ù	U grave	U
00DA	Ú	U acute	U
00DB	Û	U circumflex	U
00DC	Ü	U diaeresis	UE or UXX or U
00DD	Ý	Y acute	Y
00DE	Þ	Thorn (Iceland)	TH
0100	Ā	A macron	A
0102	Ă	A breve	A
0104	Ą	A ogonek	A
0106	Ć	C acute	C
0108	Ĉ	C circumflex	C
010A	Ċ	C dot above	C
010C	Č	C caron	C
010E	Ď	D caron	D
0110	Đ	D stroke	D

Unicode	*National character*	*Description*	*Recommended transliteration*
0112	Ē	E macron	E
0114	Ĕ	E breve	E
0116	Ė	E dot above	E
0118	Ę	E ogonek	E
011A	Ě	E caron	E
011C	Ĝ	G circumflex	G
011E	Ğ	G breve	G
0120	Ġ	G dot above	G
0122	Ģ	G cedilla	G
0124	Ĥ	H circumflex	H
0126	Ħ	H stroke	H
0128	Ĩ	I tilde	I
012A	Ī	I macron	I
012C	Ĭ	I breve	I
012E	Į	I ogonek	I
0130	İ	I dot above	I
0131	I	I without dot (Turkey)	I
0132	IJ	ligature IJ	IJ
0134	Ĵ	J circumflex	J
0136	Ķ	K cedilla	K
0139	Ĺ	L acute	L
013B	Ļ	L cedilla	L
013D	Ľ	L caron	L
013F	Ŀ	L middle dot	L
0141	Ł	L stroke	L
0143	Ń	N acute	N
0145	Ņ	N cedilla	N
0147	Ň	N caron	N
014A	Ŋ	Eng	N
014C	Ō	O macron	O
014E	Ŏ	O breve	O
0150	Ő	O double acute	O
0152	Œ	ligature OE	OE
0154	Ŕ	R acute	R
0156	Ŗ	R cedilla	R
0158	Ř	R caron	R
015A	Ś	S acute	S

Unicode	*National character*	*Description*	*Recommended transliteration*
015C	Ŝ	S circumflex	S
015E	Ş	S cedilla	S
0160	Š	S caron	S
0162	Ţ	T cedilla	T
0164	Ť	T caron	T
0166	Ŧ	T stroke	T
0168	Ũ	U tilde	U
016A	Ū	U macron	U
016C	Ŭ	U breve	U
016E	Ů	U ring above	U
0170	Ű	U double acute	U
0172	Ų	U ogonek	U
0174	Ŵ	W circumflex	W
0176	Ŷ	Y circumflex	Y
0178	Ÿ	Y diaeresis	Y
0179	Ź	Z acute	Z
017B	Ż	Z dot above	Z
017D	Ž	Z caron	Z
1E9E	ß	double s (Germany)	SS

B. Transliteration of Cyrillic Characters

Unicode	*National character*	*Recommended transliteration*
0401	Ё	E (except Belorussian = IO)
0402	Ђ	D
0404	Є	IE (except if Ukrainian first character, then =YE)
0405	S	DZ
0406	I	I
0407	Ї	I (except if Ukrainian first character, then =YI)
0408	J	J
0409	Љ	LJ
040A	Њ	NJ
040C	Ќ	K (except in the language spoken in the former Yugoslav Republic of Macedonia = KJ)
040E	ў	U
040F	Џ	DZ (except in the language spoken in the former Yugoslav Republic of Macedonia = DJ)

Unicode	*National character*	*Recommended transliteration*
0410	А	A
0411	Б	B
0412	В	V
0413	Г	G (except Belorussian, Serbian, and Ukrainian = H)
0414	Д	D
0415	Е	E
0416	Ж	ZH (except Serbian = Z)
0417	З	Z
0418	И	I (except Ukrainian = Y)
0419	Й	I (except if Ukrainian first character, then =Y)
041A	К	K
041B	Л	L
041C	М	M
041D	Н	N
041E	О	O
041F	П	P
0420	Р	R
0421	С	S
0422	Т	T
0423	У	U
0424	Ф	F
0425	Х	KH (except Serbian and in the language spoken in the former Yugoslav Republic of Macedonia = H)
0426	Ц	TS (except Serbian and in the language spoken in the former Yugoslav Republic of Macedonia = C)
0427	Ч	CH (except Serbian = C)
0428	Ш	SH (except Serbian = S)
0429	Щ	SHCH (except Bulgarian = SHT)
042A	Ъ	IE
042B	Ы	Y
042D	Э	E
042E	Ю	IU (except if Ukrainian first character, then =YU)
042F	Я	IA (except if Ukrainian first character, then =YA)
046A	Ѫ	U
0474	Ѵ	Y

Unicode	*National character*	*Recommended transliteration*
0490	Ґ	G
0492	Ғ	G (except in the language spoken in the former Yugoslav Republic of Macedonia = GJ)
04BA	Һ	C

C. Transliteration of Arabic Script

Unicode	*Arabic letter*	*Name*	*MRZ*
0621	ء	hamza	XE
0622	آ	alef with madda above	XAA
0623	أ	alef with hamza above	XAE
0624	ؤ	waw with hamza above	U
0625	إ	alef with hamza below	I
0626	ئ	yeh with hamza above	XI
0627	ا	alef	A
0628	ب	beh	B
0629	ة	teh marbuta	XTA/XAH[1]
062A	ت	teh	T
062B	ث	theh	XTH
062C	ج	jeem	J
062D	ح	hah	XH
062E	خ	khah	XKH
062F	د	dal	D
0630	ذ	thal	XDH
0631	ر	reh	R
0632	ز	zain	Z

[1] XTA is used generally except if *teh marbuta* occurs at the end of the name component, in which case XAH is used.

Unicode	*Arabic letter*	*Name*	*MRZ*
0633	س	seen	S
0634	ش	sheen	X S H
0635	ص	sad	X S S
0636	ض	dad	X D Z
0637	ط	tah	X T T
0638	ظ	zah	X Z Z
0639	ع	ain	E
063A	غ	ghain	G
0640	ـ	tatwheel	(Not encoded)
0641	ف	feh	F
0642	ق	qaf	Q
0643	ك	kaf	K
0644	ل	lam	L
0645	م	meem	M
0646	ن	noon	N
0647	ه	heh	H
0648	و	waw	W
0649	ى	alef maksura	X A Y
064A	ي	yeh	Y
064B	ً	fathatan	(Not encoded)
064C	ٌ	dammatan	(Not encoded)
064D	ٍ	kasratan	(Not encoded)
064E	َ	fatha	(Not encoded)
064F	ُ	damma	(Not encoded)
0650	ِ	kasra	(Not encoded)

Unicode	*Arabic letter*	*Name*	*MRZ*
0651	ّ	shadda	[DOUBLE][2]
0652	ْ	sukun	(Not encoded)
0670	ٰ	superscript alef	(Not encoded)
0671	آ	alef wasla	XXA
0679	ٹ	tteh	XXT
067C	ټ	teh with ring	XRT
067E	پ	peh	P
0681	ځ	hah with hamza above	XKE
0685	څ	hah with 3 dots above	XXH
0686	چ	tcheh	XC
0688	ڈ	ddal	XXD
0689	ډ	dal with ring	XDR
0691	ڑ	rreh	XXR
0693	ړ	reh with ring	XRR
0696	ږ	reh with dot below and dot above	XRX
0698	ژ	jeh	XJ
069A	ښ	seen with dot below and dot above	XXS
069C	ڜ	seen with 3 dots below and 3 dots above	(Not encoded)
06A2	ڢ	feh with dot moved below	(Not encoded)
06A7	ڧ	qaf with dot above	(Not encoded)
06A8	ڨ	qaf with 3 dots above	(Not encoded)
06A9	ک	keheh	XKK
06AB	ګ	kaf with ring	XXK
06AD	ڭ	ng	XNG
06AF	گ	gaf	XGG

2 Shadda denotes doubling: Latin character or sequence is repeated eg عبّاس becomes EBBAS; فضّة becomes FXDZXDZXAH.

Unicode	*Arabic letter*	*Name*	*MRZ*
06BA	ں	noon ghunna	XNN
06BC	ڼ	noon with ring	XXN
06BE	ھ	heh doachashmee	XDO
06C0	ۀ	heh with yeh above	XYH
06C1	ہ	heh goal	XXG
06C2	ۂ	heh goal with hamza above	XGE
06C3	ۃ	teh marbuta goal	XTG
06CC	ی	farsi yeh	XYA
06CD	ۍ	yeh with tail	XXY
06D0	ې	yeh	Y
06D2	ے	yeh barree	XYB
06D3	ۓ	yeh barree with hamza above	XBE

7. DEVIATIONS

As States worldwide continue to adopt MRTDs, the increased complexity and the rise in deviations have led to a need for reporting deviations from standards or the normal practice of a State through a standardized mechanism. Deviations are defined as MRTDs that contain elements that do not precisely conform to the ICAO specifications and the governing ISO and RFC standards. Deviations are generally observed within Country Signing Certificate Authorities (CSCA) or Document Signer Certificates (DSCs). Nonetheless, States have also indicated issues related to the LDS and MRZ fields within their MRTDs. The purpose of this section is to detail the mechanism by which issuing States can publish their deviations.

While travel documents may contain deviations, they may still be usable in border management systems. For documents that are otherwise valid, they may remain in use for several years. Consequently, relying parties should identify their own processes for handling any published deviations.

7.1 Operational Experiences

For a long time the only method for managing deviations was through the general advice given by issuing States via diplomatic means. This section includes deviations affecting large numbers of MRTDs that might be reported so as to assist borders in making a determination on whether travel documents are valid, forged or the product of a substitution. Some examples of operational errors include MRZ, LDS and PKI deviations.

While the MRZ has been in use for many years some recent examples of known MRZ errors are:

- MRZ date of birth does not match VIZ page date of birth.

- MRZ citizenship incorrectly reports the country of birth rather than citizenship.

In most cases travel documents with a non-conforming MRZ will be recalled by the issuing State. Since there is a gap between issuance and the subsequent reissuance, travellers may be forced to use their deviating MRTD. During this time, a published deviation may alleviate potential problems for travellers.[3]

For LDS and PKI deviations, some could go undetected for long periods of time, as many States are not yet performing Passive and Active Authentication as specified by Doc 9303. However, issuing States are strongly encouraged to publish deviations in order assist the global community in the technical adoption of MRTDs.[4]

7.2 Deviation List Approach

The approach described in this section aims to provide a standardized means for issuing States to publish and distribute a Travel Document Deviation List. It is based on principles established during the development of the CSCA Master List (see Doc 9303-12), in that a signed Deviation List for each State's non-conformities will be provided via the ICAO PKD or the issuing authority through a website or a LDAP-server. The PKD is used to support the dissemination of information relevant to the management of deviations.

Deviations are categorized into four specific areas:

- Keys and Certificates;
- Logical Data Structure (LDS);
- Machine Readable Zone (MRZ);
- Chip.

For each of these categories deviations will be described to one level only, for example:

Category:	LDS
Error	DG2

Additional information will be provided via an operational parameter as made available by each State and/or a free text field in the reporting framework allowing the notifying State to add any descriptive text required. The notifying State can include links to additional information within the free text field. For certificate errors, the issuer will have the option to issue a new certificate, but this will not be mandatory.

The decision to advise relying parties of a non-conformity remains solely with the issuing State. In deciding whether to create a Deviation List, States should take into consideration that as traveller self-processing border solutions become more common, failure to communicate information relevant to non-conforming travel documents may cause delays and inconvenience for travellers, which will reflect poorly on both the issuing State and the border process as a whole.

3 Non conformities that affect single documents or small numbers of eMRTDs will not be addressed by this section, it is up to the issuing State to recall and re-issue individual documents.

4 For any instance where there has been a security issue related to a PKI certificate, the proper response is revocation as described in Doc 9303-12. Further guidance is outside the scope of this section.

Deviation Lists provide a means of reporting deviations affecting thousands of travel documents rather than a few or a few hundred. It is appropriate for States to manage small numbers of non-conforming travel documents directly.

7.3 Method

7.3.1 Deviation elements

The elements that make up an MRTD range from paper to RFID chips, with each element protected in some way by security features that can be defined and thus tested by inspection systems during the life of the travel document. Security features employed on the physical travel document are both overt and covert. This section considers only deviation elements within the MRZ, LDS and PKI.

The MRZ is a fixed-dimensional area located on the MRTD data page, containing mandatory and optional data formatted for machine reading using OCR methods. Doc 9303 provides the specifications for the MRZ, including:

- purpose;
- constraints;
- transliteration; and
- data structure of the MRZ lines.

The conformity of the MRZ is routinely tested by inspection systems via data comparison with the corresponding VIZ page data and recalculation of the MRZ check digits.

The authenticity and integrity of data stored on MRTD RFID chip is protected by Passive Authentication. This security mechanism is based on digital signatures and Public Key Infrastructure (PKI).

The structure of the MRTD LDS is defined by Doc 9303-10. While there are no specific tests to establish conformity, the data stored within the LDS is in part a subset of data available from the MRZ or VIZ page of the MRTD. Consequently, the same tests apply for the digital MRZ and VIZ data as would be applied to the MRZ and VIZ page. Authenticity of the LDS is provided through the correct application of Passive Authentication by inspection systems, while Active Authentication is performed by the chip. A brief description is below:

Passive Authentication (PA) is based on digital signatures and consists of the following PKI components:

1. **Country Signing CA (CSCA):** Every State establishes a CSCA as its national trust point in the context of eMRTDs. The CSCA issues public key certificates for one or more (national) Document Signers. In addition each CSCA issues Certificate Revocation Lists (CRLs) of all revoked certificates.[5]

2. **Document Signers (DS):** A Document Signer digitally signs data to be stored on MRTDs; this signature is stored in the Document Security Object for each document.

Active Authentication (AA): Where AA is implemented, each chip contains its own AA Key Pair. The private Key is stored in the chip's secure memory with the Public Key stored at LDS Data Group 15.

5 Since CRLs are a security reporting mechanism and are constantly reissued, no defects reporting is necessary for them and they are therefore outside the scope of this Part.

7.3.2 Issuing Deviation Lists

Deviation Lists MUST NOT be issued directly by a CSCA, instead the CSCA SHALL authorize a Deviation List Signer (see Doc 9303-12) to compile, sign and publish Deviation Lists. For Deviation List specifications, see Doc 9303-12.

The procedures to be performed for issuing a Deviation List SHOULD be reflected in the published certification policies of the issuing CSCA.

7.3.3 Receiving a Deviation List

Every Receiving State defines its own policies under which it accepts a Deviation List and how deviations are handled during the inspection of documents. Those policies are, in general, private information.

The Receiving State will at its sole discretion choose to allow MRTDs with a deviation to be utilized.

7.3.4 Categories of Deviations

7.3.4.1 Keys and certificates

Certificate and key deviations are restricted to the following:

Issue	*Comment*
Certificate	Described to the Field or Extension
Keys	Described to the Field or Extension
AA	Described to the error/problem only

Note.— Where a reporting State decides to issue a new certificate, the certificate MUST NOT be included in the Deviation List, but could be pointed to via the free text field.

7.3.4.2 Logical Data Structure (LDS)

LDS deviations are restricted to the following:

Issue	*Comment*
EF.Com	Described to the encoding error
DG’s	Described to the Data Group
EF.sod	Described to the issue (e.g. DSC)

7.3.4.3 Machine Readable Zone (MRZ)

MRZ deviations are restricted to the following:

Issue	*Comment*
Match to VIZ	Described to the field
Check Digits	Described to the responsible check digit
Wrong Information encoded	Described to the MRZ field

7.3.5 Deviation type definitions

Categories of deviations and corresponding parameters may be extended over time and will be maintained in Doc 9303.

Each deviation is described by a deviationDescription element. The deviation is identified by an Object Identifier deviationType and may be further detailed by parameters. The field description MAY contain further information, such as how the nature of the deviation cannot be adequately described by the governing deviationType.

DeviationType	Parameters	Description
Certificate/Key Deviation		
`id-Deviation-CertOrKey`	None	A generic certificate or key related deviation not covered by the more detailed deviations below.
`id-Deviation-CertOrKey-DSSignature`	None	The signature of the Document Signer Certificate is wrong.
`id-Deviation-CertOrKey-DSEncoding CertField`	`CertField`	The Document Signer Certificate contains a coding error.
`id-Deviation-CertOrKey-CSCAEncoding`	`CertField`	The Country Signing CA Certificate contains a coding error.
`id-Deviation-CertOrKey-AAKeyCompromised`	None	The key for Active Authentication may be compromised and should not be relied upon.
LDS Deviation		
`id-Deviation-LDS`	None	A generic LDS related deviation not covered by the more detailed deviations below.
`id-Deviation-LDS-DGMalformed`	`Datagroup`	The TLV encoding of the given datagroup is corrupted.
`id-Deviation-LDS-DGHashWrong`	`Datagroup`	The hash value of the given datagroup in the EF.SOD is wrong.
`id-Deviation-LDS-SODSignatureWrong`	None	The signature contained in EF.SOD is wrong.
`id-Deviation-LDS-COMinconsistent`	None	EF.COM and EF.SOD are inconsistent.

DeviationType	Parameters	Description
MRZ Deviation		
`id-Deviation-MRZ`	None	A generic MRZ related deviation not covered by the more detailed deviation below.
`id-Deviation-MRZ-WrongData`	MRZField	The given field of the MRZ contains wrong data (e.g. inconsistent with VIZ), but the derived BAC key is usable to open the chip. If the derived BAC key is not usable, additionally id-Deviation-Chip SHALL be included in the Deviation List.
`id-Deviation-MRZ-WrongCheckDigit`	MRZField	The check digit to given field of the MRZ is calculated wrong.
Chip Deviation		
`id-Deviation-Chip`	None	The Chip is not usable, e.g. wrong BAC key, broken antenna or other physical defect.

ICAO Object Identifiers are specified in 9303-10, 9303-11, and 9303-12. A list of the Deviation Object Identifiers follows:

```
-- Deviation List Base Object identifiers
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 7}

id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 8}


-- Deviation Object Identifiers and Parameter Definitions
id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 2}

id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-
CertOrKey 3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-
Deviation-CertOrKey 4}

id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}
```

```
id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS
3}

id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}
```

7.3.6 Identification of deviant documents

Documents affected by a deviation MAY be identified by several different means:

- by the Document Signer Certificate used to sign these documents; the Document Signer can be either identified by:
  - the Distinguished Name of the Issuer in combination with the Serial Number of the certificate (`issuerAndSerialNumber`),
  - the `subjectKeyIdentifier` uniquely identifying the Document Signer, or
  - the hash of the Document Signer certificate (`certificateHash`); the hash function to be used is the same as used in the signature of the Deviation List.
- by a range of issuing dates (`startIssuingDate, endIssuingDate`)
- by a list of document numbers (`listOfDocNumbers`).

Each method has advantages and disadvantages for the issuer of a Deviation List as well for the receiver of a Deviation List. These include:

- Identification by Document Signer allows recognition of a deviation by the inspection systems only after Passive Authentication was performed. Additionally, identification by Document Signer might be too coarse to accurately identify only defect documents, i.e. the deviation affects only part of the documents signed by a given Document Signer.
- The Issuing Date is not part of the machine readable zone, and also in general not available in the electronic LDS. Therefore this is not suitable for automated processing. Additionally, depending on the Issuing State, the Issuing Date might not be the actual date of passport personalization, but the application date, and therefore not accurate enough to identify only affected documents.
- A list of document numbers is difficult to compile if document numbers are not issued sequentially. A list of document numbers grows quite quickly to unmanageable size if many documents are affected by a defect.

It is RECOMMENDED to give as much identifying information on affected documents as possible. If several methods for identification are given, the conditions MUST be met simultaneously to identify a document. It is at the discretion of the

Relying State to decide which means of identification given in a Deviation List entry are used to identify affected documents.

7.4 Publication

Deviation Lists can be published via the ICAO PKD and/or the issuing authority through a website or LDAP server. The primary distribution point for DeviationLists is the PKD.

	Deviation Lists
Primary Distribution	PKD
Secondary Distribution	Website/LDAP

7.4.1 Publication by the issuing State

Deviation Lists can be published via a website or an LDAP-server of the issuing authority.

7.4.2 Publication on the PKD

The PKD operates as a central repository for Deviation Lists.

The procedure for publishing a Deviation List is as follows:

1. Deviation Lists are sent to the write PKD, as part of the usual certificate upload process as defined in the PKD Interface Specification and PKD Procedures Manual.

2. The ICAO PKD office validates the signatures of uploaded Deviation Lists as specified in the PKD Procedures Manual.

3. Valid Deviation Lists are moved to the read PKD.

4. The distributing State will determine if its Deviation List will be publicly available, or restricted to PKD member States.

7.4.3 Relying parties

To be able to verify a Deviation List, a relying party needs to have received the corresponding CSCA certificate of the issuing State by out-of-band communications. It is up to the Relying Party to decide how to handle MRTDs with a corresponding entry in the issuing State's Deviation List.

8. REFERENCES (NORMATIVE)

[ISO 1073-2] ISO 1073-2:1976, Alphanumeric character sets for optical recognition – Part 2: Character set OCR-B – Shapes and dimensions of the printed image

[ISO 1831] ISO 1831:1980, Printing specifications for optical character recognition

[ISO 1664-2] ISO 11664-2:2007(E)/CIE S014-2/E: 2006, CIE Standard Illuminants for Colorimetry

[ISO 12233] ISO 12233: Photography – Electronic still picture imaging – Resolution and spatial frequency responses

[ISO 3166-1] ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions – Part 1:Country codes

[ISO 3166/MA] ISO 3166 Maintenance Agency https://www.iso.org/iso/home/standards/country_codes.htm

[ISO/IEC 7810] ISO/IEC 7810:2003, Identification cards – Physical characteristics

[ISO/IEC 39794-5] ISO/IEC 39794-5:2019, Extensible biometric data interchange formats— Part 5: Face image data

[ISO/IEC 7501] ISO/IEC 7501 multipart standard: Machine Readable Travel Documents

[ISO/IEC 10918-1] ISO/IEC 10918-1:1994, Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines

[ISO/IEC 15444-1] ISO/IEC 15444-1:2004, Information technology - JPEG 2000 image coding system: Core coding system

[ISO/IEC 15948] ISO/IEC 15948:2004, Information technology – Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification

[ISO/IEC 14496-2] ISO/IEC 14496-2 Information technology – Coding of audio-visual objects Part 2: Visual [MPEG4]

[IEC 61966-2-1] IEC 61966-2-1: Multimedia systems and equipment – Colour measurement and management – Part 2-1: Colour management – Default RGB colour space – sRGB

[IEC 61966-8] IEC 61966-8:2001, Multimedia systems and equipment – Colour measurement and management – Part 8: Multimedia colour scanners

[TR-03121-3] BSI: Technical Guideline TR-03121-3: Biometrics for public sector applications, Part 3: Application Profiles and Function Modules, Volume 1: Verification scenarios for ePassport and Identity Card, Version 3.0.1. 2013

[RFC 3852] Cryptographic Message Syntax – July 2004

[RFC 5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“, May 2008

— — — — — — — —

APPENDIX A TO PART 3 —EXAMPLES OF CHECK DIGIT CALCULATION (INFORMATIVE)

Example 1 — Application of check digit to date field

Using 27 July 1952 as an example, with the date in numeric form, the calculation will be:

	Date:	5	2	0	7	2	7
	Weighting:	7	3	1	7	3	1
Step 1 (multiplication)	Products:	35	6	0	49	6	7

Step 2 (sum of products) 35 + 6 + 0 + 49 + 6 + 7 = 103

Step 3 (division by modulus) $\frac{103}{10}$ = 10, remainder 3

Step 4. Check digit is the remainder, 3. The date and its check digit shall consequently be written as `5207273`.

Example 2 — Application of check digit to document number field

Using the number AB2134 as an example for coding a 9-character, fixed-length field (e.g. passport number), the calculation will be:

Sample data element:	A	B	2	1	3	4	<	<	<
Assigned numeric values:	10	11	2	1	3	4	0	0	0
Weighting:	7	3	1	7	3	1	7	3	1
Step 1 (multiplication) Products:	70	33	2	7	9	4	0	0	0

Step 2 (sum of products) 70 + 33 + 2 + 7 + 9 + 4 + 0 + 0 + 0 = 125

Step 3 (division by modulus) $\frac{125}{10}$ = 12, remainder 5

Step 4. Check digit is the remainder, 5. The number and its check digit shall consequently be written as `AB2134<<<5`.

Examples of the calculation of composite check digits.

The calculation method for composite check digits is the same for all MRTDs. However, the location and number of the digits to be included in the calculation are different between the different types of documents. For completeness, examples of each are included here.

Example 3 — Composite check digit calculation for TD3 documents

Using the lower line of MRZ data from a TD3 data page that follows, as an example for coding the composite check digit, the calculation will be:

Character positions 1-43: Example with no alpha-numeric characters in “optional data” field.

HA672242<6YT05802254M9601086<<<<<<<<<<<<<<0

Sample data element:	H	A	6	7	2	2	4	2	<	6
Assigned numeric values:	17	10	6	7	2	2	4	2	0	6
Weighting:	7	3	1	7	3	1	7	3	1	7
Step 1 (multiplication) Products:	119	30	6	49	6	2	28	6	0	42

Sample data element:	5	8	0	2	2	5	4	9	6	0
Assigned numeric values:	5	8	0	2	2	5	4	9	6	0
Weighting:	3	1	7	3	1	7	3	1	7	3
Step 1 (multiplication) Products:	15	8	0	6	2	35	12	9	42	0

Sample data element:	1	0	8	6	<	<	<	<	<	<
Assigned numeric values:	1	0	8	6	0	0	0	0	0	0
Weighting:	1	7	3	1	7	3	1	7	3	1
Step 1 (multiplication) Products:	1	0	24	6	0	0	0	0	0	0

Sample data element:	<	<	<	<	<	<	<	<	0	
Assigned numeric values:	0	0	0	0	0	0	0	0	0	
Weighting:	7	3	1	7	3	1	7	3	1	
Step 1 (multiplication) Products:	0	0	0	0	0	0	0	0	0	

Step 2 (sum of products)	119	+	30	+	6	+	49	+	6	+	2	+	28	+	6	+	0	+	42
Step 2 (sum of products)	15	+	8	+	0	+	6	+	2	+	35	+	12	+	9	+	42	+	0
Step 2 (sum of products)	1	+	0	+	24	+	6	+	0	+	0	+	0	+	0	+	0	+	0
Step 2 (sum of products)	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0		
Step 2 (sum of products)	448																		
Step 3 (division by modulus)	448 = 44, remainder 8																		

10

Step 4. Check digit is the remainder, 8. The lower line of MRZ data together with its composite check digit may consequently be written as follows:

HA672242<6YT05802254M9601086<<<<<<<<<<<<<<08

Example 4 — Composite check digit calculation for TD1 documents

Using the upper and middle lines of MRZ data of a TD1 that follow as an example for coding the composite check digit, the calculation will be:

Upper machine readable line (character positions 1–30): I<YTOD231458907<<<<<<<<<<<<<<<

Middle machine readable line (character positions 1–29): 3407127M9507122YTO<<<<<<<<<<<

Sample data element:	D	2	3	1	4	5	8	9	0	7
Assigned numeric values:	13	2	3	1	4	5	8	9	0	7
Weighting:	7	3	1	7	3	1	7	3	1	7
Step 1 (multiplication) Products:	91	6	3	7	12	5	56	27	0	49

Sample data element:	<	<	<	<	<	<	<	<	<	<
Assigned numeric values:	0	0	0	0	0	0	0	0	0	0
Weighting:	3	1	7	3	1	7	3	1	7	3
Step 1 (multiplication) Products:	0	0	0	0	0	0	0	0	0	0

Sample data element:	<	<	<	<	<
Assigned numeric values:	0	0	0	0	0
Weighting:	1	7	3	1	7
Step 1 (multiplication) Products:	0	0	0	0	0

Sample data element:	3	4	0	7	1	2	7	9	5	0
Assigned numeric values:	3	4	0	7	1	2	7	9	5	0
Weighting:	3	1	7	3	1	7	3	1	7	3
Step 1 (multiplication) Products:	9	4	0	21	1	14	21	9	35	0

Sample data element:	7	1	2	2	<	<	<	<	<	<
Assigned numeric values:	7	1	2	2	0	0	0	0	0	0
Weighting:	1	7	3	1	7	3	1	7	3	1
Step 1 (multiplication) Products:	7	7	6	2	0					

Sample data element:	<	<	<	<	<
Assigned numeric values:	0	0	0	0	0
Weighting:	7	3	1	7	3
Step 1 (multiplication) Products:	0	0	0	0	0

Step 2 (sum of products)	91 + 6 + 3 + 7 + 12 + 5 + 56 + 27 + 0 + 49 +
Step 2 (sum of products)	0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 +
Step 2 (sum of products)	0 + 0 + 0 + 0 + 0 + 9 + 4 + 0 + 21 + 1 +
Step 2 (sum of products)	14 + 21 + 9 + 35 + 0 + 7 + 7 + 6 + 2 + 0 +
Step 2 (sum of products)	0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0
Step 2 (sum of products)	= 392
Step 3 (division by modulus)	392 = 39, remainder 2 10

Step 4. Check digit is the remainder, 2. The middle line of MRZ data together with its composite check digit may consequently be written as follows: `3407127M9507122YTO<<<<<<<<<<<2`.

Example 5 — Composite check digit calculation for TD2 documents.

Using the lower line of MRZ data that follows as an example for coding the composite check digit, the calculation will be:
Lower machine readable line (character positions 1–35):

`HA672242<6YT05802254M9601086<<<<<<<`

Sample data element:	H	A	6	7	2	2	4	2	<	6
Assigned numeric values:	17	10	6	7	2	2	4	2	0	6
Weighting:	7	3	1	7	3	1	7	3	1	7
Step 1 (multiplication) Products:	119	30	6	49	6	2	28	6	0	42

Sample data element:	5	8	0	2	2	5	4	9	6	0
Assigned numeric values:	5	8	0	2	2	5	4	9	6	0
Weighting:	3	1	7	3	1	7	3	1	7	3
Step 1 (multiplication) Products:	15	8	0	6	2	35	12	9	42	0

Sample data element:	1	0	8	6	<	<	<	<	<	<
Assigned numeric values:	1	0	8	6	0	0	0	0	0	0
Weighting:	1	7	3	1	7	3	1	7	3	1
Step 1 (multiplication) Products:	1	0	24	6	0	0	0	0	0	0

Sample data element:	<
Assigned numeric values:	0
Weighting:	7
Step 1 (multiplication) Products:	0

Step 2 (sum of products) 119 + 30 + 6 + 49 + 6 + 2 + 28 + 6 + 0 + 42 +

Step 2 (sum of products) 15 + 8 + 0 + 6 + 2 + 35 + 12 + 9 + 42 + 0 +

Step 2 (sum of products) 1 + 0 + 24 + 6 + 0 + 0 + 0 + 0 + 0 + 0 +

Step 2 (sum of products) 0

Step 2 (sum of products) = 448

Step 3 (division by modulus) $\frac{448}{10}$ = 44, remainder 8

Step 4. Check digit is the remainder, 8. The lower line of MRZ data together with its composite check digit may consequently be written as follows:

HA672242<6YT05802254M9601086<<<<<<<8.

— — — — — — — —

APPENDIX B TO PART 3 — TRANSLITERATION OF ARABIC SCRIPT IN MRTDS (INFORMATIVE)

B.1 The Arabic Script

The Arabic script is used by the Arabic language, the official language of about 24 countries from Morocco to Oman. The Arabic script is also used by other languages, notably Farsi in Iran; Pashto and Dari in Afghanistan; Urdu in Pakistan; and many others, including Kurdish, Assyrian, Hausa and Uighur. In the past it was used for the languages of Central Asia, for example, Tajik and Uzbek.

The Arabic script is cursive, and a letter will often change its shape depending upon whether it is standing alone (isolated); at the start of a word (initial); in the body of a word (medial); or at the end (final). For example, the letter ب(beh) changes its shape to بـ at the beginning of the word بكر (Bakr) — note that Arabic reads from right to left, so the first letter is at the right hand side. We are not concerned here with these different letter shapes (glyphs), only the basic letter code — represented by the isolated shape.

Arabic and the other languages using the Arabic script are usually written using consonants alone. Thus the name محمد (Mohammed) as written consists of just four consonants, which may be approximated in Latin as "Mhmd". The vowels are added at the discretion of the translator to achieve a phonetic equivalent. Arabic can also be "vocalized" if the vowel marks ("harakat") are added to modify the pronunciation. However, the harakat are normally omitted.

The standard Arabic script consists of 32 consonants, 18 vowels and dipthongs and three other signs. In addition there are over 100 national characters in the Arabic script when used with non-Arabic languages, although some of these are obsolete and no longer in use.

B.2 The Arabic Script in the MRTD

B.2.1 VIZ

The VIZ has a mandatory field for the name (refer to specifications for each form factor in Doc 9303, Parts 4 through 7). Doc 9303-3, paragraph 3.1, states:

> *"When mandatory data elements are in a language that does not use the Latin alphabet, a transliteration shall also be provided."*

Thus if the name is written in the Arabic script, a Latin representation shall be included. While Doc 9303 refers to this representation as a "transliteration", it is commonly a phonetic equivalent and should be more correctly termed a "transcription".

For example:

the name[1] in Arabic script: **ابو بكر محمد بن زكريا الرازي**

and a transcription into Latin characters: **Abū Bakr Mohammed ibn Zakarīa al-Rāzi**

Firstly note that Doc 9303-3, paragraph 3.2, allows the use of diacritical marks (e.g. the **ā** in **al-Rāzi**) in the VIZ at the option of the issuing State.

Secondly, note that this particular transcription into Latin characters is only one of many possibilities. The "Database of Arabic Name Variants" website[2] gives the following sixteen variations for **محمد**:

1. Muhammad
2. Moohammad
3. Moohamad
4. Mohammad
5. Mohamad
6. Muhamad
7. Muhamad
8. Mohamed
9. Mohammed
10. Mohemmed
11. Mohemmed
12. Muhemmed
13. Muhamed
14. Muhammed
15. Moohammed
16. Mouhammed

In some countries it is common to replace the final "d" with "t", so this leads to a total of 32 variations for **محمد**.

The transcription scheme used depends upon the language and regional accent of the Arabic script source (non-Arabic languages such as Farsi, Pashto and Urdu also use the Arabic script); the language of the Latin script speaker; and the transcription scheme used.

B.2.2 MRZ

Section 4 of this part of Doc 9303 describes the MRZ.

The MRZ provides a set of essential data elements in a format standardized for each type of MRTD that can be used by all receiving States regardless of their national script or customs. The data in the MRZ are formatted in such a way as to be readable by machines with standard capability worldwide and, as a consequence, the MRZ is a different representation of the data than is found in the VIZ. National characters generally appear only in the computer-processing systems of the States in which they apply and are not available globally. They shall not, therefore, appear in the MRZ.

The Name Field of the MRZ consists, in the case of the MRP, of 39 character positions, and only the OCR-B subset of A-Z and < may be used. Thus Arabic characters shall not be used in the MRZ, and "equivalent" OCR-B characters must be used to represent them.

The conversion of the name in the Arabic script to the Latin characters of the MRZ, constrained by the use of only the OCR-B characters A-Z and <, is problematical. In addition, the uncertainty introduced if a phonetic-based transcription is allowed means that database searches can become useless.

For example, from the same example used above:

the name in Arabic script: **ابو بكر محمد بن زكريا الرازي**

[1] Abū Bakr al-Rāzi was a great Persian scientist and doctor of about 1 100 years ago. In Persian (Farsi), his name is usually spelt with a final Persian "yeh" (ى), but to avoid confusion we have used the standard Arabic "yeh" (ي).

[2] See <http://www.kanji.org/cjk/arabic/araborth.htm>.

and one **transcription** into Latin characters for the MRZ:

ABU<BAKR<MOHAMMED<IBN<ZAKARIA<AL<RAZI

However the MRZ is likely to be one of at least 32 variants based on the name “Mohammed” alone. “Zakaria” may be written “Zakariya”; “ibn” as “bin”; and “al” as “el”. Just these variations lead to 256 alternatives.

To draw the contrast, a **transliteration** of the above name **محمد**, for example, applying the Buckwalter table (see below) to the four Arabic characters, would be “mHmd”. In this case, each Arabic character maps into a single Latin character. No allowance is made for phonetics.

The complete Buckwalter transliteration of the name above is:

Abw<bAkr<mHmd<bn<zkryAY<AlrAzY

Unfortunately, the Buckwalter table uses lower case (a-z) and special characters (‘,|,>,$,<,},*,_,~) so is not suitable for use in the MRZ (see http://www.qamus.org/transliteration.htm).

B.3 Recommendation for the VIZ

B.3.1 Transcription in the VIZ

As stated above, Doc 9303-3, paragraph 3.1, mandates the inclusion of a “transliteration” in the VIZ when a national script other than Latin is used. Related Doc 9303-3, paragraph 3.4, refers specifically to the requirement for names.

There is confusion about the terms “transliteration” and “transcription”. A “transliteration” is a strictly one-to-one representation of the non-Latin script. A “transcription” is a more loose representation, often based on phonetics (how the name “sounds” when spoken). Of course, often sounds made in one language do not have equivalents in another, and it depends on the target language, for example, “ch”, “sh” and “th” are pronounced differently in English and French and German. Compare the English transcription “Omar Khayyam” with the German transcription “Omar Chajjam” for the name of the mathematician and poet **عمر خيام**.

There are many “transcription” schemes:

- Deutches Institut für Normung: DIN 31635 (1982)
- Deutsche Morgenländische Gesellschaft (1936)
- International Standards Organisation: ISO/R 233 (1961), ISO 233 (1984)[3], ISO 233-2 (1993)
- British Standards Institute: BS 4280 (1968)
- United Nations Group of Experts on Geographical Names (UNGEGN): UN (1972) [4]
- Qalam (1985)
- American Library Association – Library of Congress: ALA-LC (1997) [1]
- The Encyclopedia of Islam, new edition: EI (1960) [2]

Some countries maintain their citizens’ names in birth or citizen registers in both Arabic and Latin script, where the Latin version is an approved transcription of the Arabic version. These countries may wish to continue to enter the approved Latin transcription in the VIZ.

Recommendation

Doc 9303-3, in paragraphs 3.1 and 3.4 as stated above, makes it mandatory to provide a Latin character equivalent in the VIZ, so it is at the discretion of the issuing State as to whether this is a phonetic transcription, or a copy of the MRZ transliteration (as described below).

B.3.2 Transcription schemes

Some of the transcription schemes are presented below:

Unicode	*Arabic letter*	*Name*[3]	*DIN 31635*	*ISO 233*	*UN GEGN*	*ALA-LC*	*EI*
0621	ء	hamza	'	'	'	'	'
0622	آ	alef with madda above	'ā	'â	ā	ā	Ā
0627	ا	alef	Ā	'			
0628	ب	beh	B	b	b	b	B
0629	ة	teh marbuta	h,t	ṫ	h,t	h,t	a,at
062A	ت	teh	T	t	t	t	T
062B	ث	theh	T	ţ	th	th	Th
062C	ج	jeem	Ğ	ğ	j	j	Dj
062D	ح	hah	ḥ	ḥ	ẖ	ḥ	ḥ
062E	خ	khah	ḫ	h	kh	kh	Kh
062F	د	dal	D	d	d	d	D
0630	ذ	thal	D	d	dh	dh	Dh
0631	ر	reh	R	r	r	r	R
0632	ز	zain	Z	z	z	z	Z
0633	س	seen	S	s	s	s	S
0634	ش	sheen	Š	š	sh	sh	Sh
0635	ص	sad	ṣ	ṣ	ṣ	ṣ	ṣ
0636	ض	dad	ḍ	ḍ	ḍ	ḍ	ḍ
0637	ط	tah	ṭ	ṭ	ţ	ṭ	ṭ
0638	ظ	zah	ẓ	ẓ	ẕ	ẓ	ẓ
0639	ع	ain	'	'	'	'	'
063A	غ	ghain	Ġ	ġ	gh	gh	Gh
0640	ـ	tatwheel	[graphic filler, not transcribed]				
0641	ف	feh	F	f	f	f	F
0642	ق	qaf	Q	q	q	q	ķ
0643	ك	kaf	K	k	k	k	K
0644	ل	lam	L	l	l	l	L
0645	م	meem	M	m	m	m	M
0646	ن	noon	N	n	n	n	N
0647	ه	heh	H	h	h	h	H
0648	و	waw	W	w	w	w	W

[3] The name of the character as given in Unicode and ISO/IEC 10646.

Unicode	*Arabic letter*	*Name*[3]	*DIN 31635*	*ISO 233*	*UN GEGN*	*ALA-LC*	*EI*
0649	ى	alef maksura	Ā	ỳ	y	y	Ā
064A	ي	yeh	Y	y	y	y	Y
064B	ً	fathatan	An	á'	a	an	
064C	ٌ	dammatan	Un	ú	u	un	
064D	ٍ	kasratan	In	í	i	in	
064E	َ	fatha	A	a	a	a	A
064F	ُ	damma	u	u	u	u	U
0650	ِ	kasra	i	i	i	i	I
0651	ّ	shadda	[double]	‾	[double]	[double]	[double]
0652	ْ	sukun		º			
0670	ٰ	superscript alef	ā	ā	ā	ā	Ā

Other national characters are:

067E	پ	peh	p			p	P
0686	چ	tcheh	č			ch,zh	Č
0698	ژ	jeh	ž			zh	Zh
06A2[4]	ڢ	feh with dot moved below	f	f		q	
06A4	ڤ	veh	v			v	
06A5	ڥ	feh with 3 dots below	v			v	
06A7[4]	ڧ	qaf with dot above	q	q		f	
06A8[4]	ڨ	qaf with 3 dots above	v			v	
06AD	ڭ	ng	G			g	G
06AF	گ	gaf	G			g	G

B.4 Transliteration in the MRZ

B.4.1 Transliteration of European languages in the MRZ

It is worth considering the situation of the national characters of European languages. Doc 9303-3, Section 6 “Transliterations Recommended for use by States” includes a table: *Transliteration of Multinational Latin-based Characters*.

Most of the national characters have their diacritical marks omitted for inclusion in the MRZ. There are a group of nine characters that are treated specially, for example, the character “Ñ” can be transliterated into the MRZ as “NXX”, thus preserving its uniqueness and importance for database searches.

[4] Obsolete characters

For example:

the name in a European national script: **Térèsa CAÑON**

and the transliteration into the MRZ: CANXXON<<TERESA

While the MRZ representation appears unaesthetic (and may lead to complaints), the purpose is for machine reading, thus enabling the original name to be recovered for database searches and the like. Thus the MRZ results in the name being recognized as **CAÑON** as distinct from **CANON.**

B.4.2 Use of UNICODE

Internally, computers use encoding schemes to represent the characters of different languages. A common encoding scheme is UNICODE, which is nearly equivalent to the ISO/IEC standard 10646 (UNICODE character indices are used in the tables below).

Representations of all the characters of the Arabic script can be found in UNICODE. The UNICODE character indices are usually given as a four-digit hexadecimal number (hexadecimal is base 16, and uses the numerals 0-9 and letters A-F to represent the 16 possible numbers). All Arabic characters are located in row 06 which forms the first two digits of the numbers (i.e. 06XX).

For example:

ابو بكر محمد بن زكريا الرازي

can be encoded in UNICODE as:

ابو	Alef (ا) - Beh (ب) - Waw (و) => 0627 + 0628 + 0648
بكر	Beh (ب) – Kaf (ك) - Reh (ر) => 0628 + 0643 + 0631
محمد	Meem (م) – Hah (ح) – Meem (م) – Dal (د) => 0645 + 062D + 0645 + 062F
بن	Beh (ب) – Noon (ن) => 0628 + 0646
زكريا	Zain (ز) – Kaf (ك) – Reh (ر) – Yeh (ي) – Alef (ا) => 0632 + 0643 + 0631 + 064A + 0627
الرازي	Alef (ا) – Lam (ل) – Reh (ر) – Alef (ا) – Zain (ز) - Yeh (ي) => 0627 + 0644 + 0631 + 0627 + 0632 + 064A

B.5 Recommendation for the MRZ

B.5.1 Factors affecting transliteration in the MRZ

Doc 9303-3, paragraph 4.1 states, "... the MRZ provides verification of the information in the VIZ and may be used to provide search characters for a database inquiry." Paragraph 4.1 also states that "The data in the MRZ are formatted in such a way as to be readable by machines with standard capability worldwide", and "The MRZ is a different representation of the data than is found in the VIZ." However, in paragraph 4.2 it is stated that "the data in the MRZ must be visually readable as well as machine readable."

The aim here is to transliterate the Arabic name into equivalent Latin characters in the MRZ such that there is only one possible representation for the name. This is necessary to avoid ambiguity and make database and alert list searching as accurate as possible for reliable identification. At the same time, the MRZ must be as far as possible a recognizable representation of the name as displayed in the VIZ so that it is visually readable for the purposes of advanced passenger processing and similar uses.

B.5.2 Existing transliteration schemes

There are several transliteration schemes in use: Standard Arabic Technical Transliteration System (SATTS), Buckwalter and ASMO 449. These are presented below:

Unicode	*Arabic letter*	*Name*	*SATTS*	*Buckwalter*	*ASMO 449*
0621	ء	hamza	E	'	A
0622	آ	alef with madda above	(missing)	|	B
0623	أ	alef with hamza above	(missing)	>	C
0624	ؤ	waw with hamza above	(missing)	&	D
0625	إ	alef with hamza below	(missing)	<	E
0626	ئ	yeh with hamza above	(missing)	}	F
0627	ا	alef	A	A	G
0628	ب	beh	B	b	H
0629	ة	teh marbuta	?	p	I
062A	ت	teh	T	t	J
062B	ث	theh	C	v	K
062C	ج	jeem	J	j	L
062D	ح	hah	H	H	M
062E	خ	khah	O	x	N
062F	د	dal	D	d	O
0630	ذ	thal	Z	*	P
0631	ر	reh	R	r	Q
0632	ز	zain	;	z	R
0633	س	seen	S	s	S
0634	ش	sheen	:	$	T
0635	ص	sad	X	S	U
0636	ض	dad	V	D	V
0637	ط	tah	U	T	W
0638	ظ	zah	Y	Z	X
0639	ع	ain	"	E	Y
063A	غ	ghain	G	g	Z
0640	ـ	tatwheel	(missing)	_	0x60
0641	ف	feh	F	f	A
0642	ق	qaf	Q	q	B
0643	ك	kaf	K	k	C
0644	ل	lam	L	l	D
0645	م	meem	M	m	E
0646	ن	noon	N	n	F
0647	ه	heh	?	h	G
0648	و	waw	W	w	H
0649	ى	alef maksura	(missing)	Y	I
064A	ي	yeh	I	y	J

Unicode	*Arabic letter*	*Name*	*SATTS*	*Buckwalter*	*ASMO 449*
064B	ً	fathatan	(missing)	F	K
064C	ٌ	dammatan	(missing)	N	L
064D	ٍ	kasratan	(missing)	K	M
064E	َ	fatha	(missing)	a	N
064F	ُ	damma	(missing)	u	O
0650	ِ	kasra	(missing)	i	P
0651	ّ	shadda	(missing)	~	Q
0652	ْ	sukun	(missing)	o	R
0670	ٰ	superscript alef	(missing)	`	(missing)

As can be seen from inspection of the tables, these schemes use Latin characters outside of the range A-Z, so are fundamentally unsuitable for use in the MRZ.

The ASMO 449 scheme has an arbitrary allocation of Latin characters, whereas Buckwalter approximates some of the phonetic equivalents.

SATTS does not distinguish between heh (ه) and teh marbuta (ة), or between final yeh (ي) and alif maksura (ى), and it cannot transliterate an alif madda (آ).

B.5.3 Other considerations

The recommended transliteration scheme cannot be put forward without considering the environment in which the MRTD operates. In particular, the name in the MRZ should be as close as possible in appearance and form as the name derived from other sources. The Passenger Name Record (PNR) used by airlines and forwarded to immigration authorities in Advanced Passenger Information (API) schemes is one example. While the transliteration in the MRZ will almost always not be exactly the same as the transcription in the VIZ (and other phonetic derivatives such as the PNR), the scheme recommended here attempts to make the names in the two zones recognizably similar.

For this purpose the character ‘X’ is used as an “escape” character in the same sense as in the Transliteration of Multinational Latin-based Characters table, except only one ‘X’ is used, and it is used before the character it modifies rather than after (e.g. “XTH” versus “NXX”). One or two characters follow each ‘X’ to represent one Arabic letter. This use of ‘X’ is possible as ‘X’ does not exist in the existing transcription and transliteration schemes for Arabic.

[The difference in the usage of ‘X’ in Arabic and Latin-based transliteration is unlikely to cause confusion. For the proper application of reverse transliteration, the original script must be defined, preferably based on the country of issue.]

In some transliteration entries, a second ‘X’ is used after the initial ‘X’: for example, alef with madda above آ is “XAA”, alef wasla ٱ is “XXA”. This technique is used primarily to avoid introducing other characters which would make the MRZ less readable by humans.

The intention is that human operators viewing the raw MRZ data from existing systems will be instructed to ignore any ‘X’ characters. The resulting name should resemble that from other sources. The raw MRZ data will also be lacking vowels that would normally be included in the VIZ transcription and in other sources such as the PNR. However if human operators are instructed that the vowels are missing then the MRZ data should be regarded as a fair representation of the transcribed phonetic version.

The transliteration will also not encompass the assimilation (sandhi) of the article before the “sun letters” as this is essentially a phonetic feature, and hence the spelling may not match the phonetic transcription of the VIZ (for example, “AL-RAZI” may be “AR-RAZI” in the VIZ).

The “shadda” (symbol to denote doubling of letters) results in the denoted character being repeated in the MRZ (doubled). Search algorithms should take into account that the “shadda” may not always be present.

B.5.4 Recommended transliteration scheme for Standard Arabic

Using the Buckwalter transliteration table as a base, and taking into account the common phonetic equivalents listed in the transcription schemes (paragraph B.3.2), a recommended transliteration scheme that uses only the Latin characters A-Z can be formulated. As there is a precedent of using ‘X’ for variations (paragraph B.5.3), the character ‘X’ is used as an “escape” character to denote that the one or two characters that follow the ‘X’ represent a single Arabic letter.

Unicode	*Arabic letter*	*Name*	*MRZ*	*Comments*
0621	ء	hamza	XE	
0622	آ	alef with madda above	XAA	B.5.5.1
0623	أ	alef with hamza above	XAE	B.5.5.2
0624	ؤ	waw with hamza above	U	B.5.5.3
0625	إ	alef with hamza below	I	B.5.5.4
0626	ئ	yeh with hamza above	XI	B.5.5.5
0627	ا	alef	A	
0628	ب	beh	B	
0629	ة	teh marbuta	XTA/XAH	B.5.5.6
062A	ت	teh	T	
062B	ث	theh	XTH	
062C	ج	jeem	J	
062D	ح	hah	XH	B.5.5.7
062E	خ	khah	XKH	
062F	د	dal	D	
0630	ذ	thal	XDH	
0631	ر	reh	R	
0632	ز	zain	Z	
0633	س	seen	S	
0634	ش	sheen	XSH	
0635	ص	sad	XSS	
0636	ض	dad	XDZ	
0637	ط	tah	XTT	
0638	ظ	zah	XZZ	
0639	ع	ain	E	
063A	غ	ghain	G	
0640	ـ	tatwheel	(note 1)	B.5.5.8
0641	ف	feh	F	
0642	ق	qaf	Q	
0643	ك	kaf	K	
0644	ل	lam	L	
0645	م	meem	M	
0646	ن	noon	N	
0647	ه	heh	H	B.5.5.7
0648	و	waw	W	
0649	ى	alef maksura	XAY	B.5.5.9
064A	ي	yeh	Y	

Unicode	*Arabic letter*	*Name*	*MRZ*	*Comments*
064B	ً	fathatan	(note 1)	B.5.5.10
064C	ٌ	dammatan	(note 1)	B.5.5.10
064D	ٍ	kasratan	(note 1)	B.5.5.10
064E	َ	fatha	(note 1)	B.5.5.10
064F	ُ	damma	(note 1)	B.5.5.10
0650	ِ	kasra	(note 1)	B.5.5.10
0651	ّ	shadda	(doubling)	B.5.5.11
0652	ْ	sukun	(note 1)	B.5.5.12
0670	ٰ	superscript alef	(note 1)	B.5.5.13
0671	ٱ	alef wasla	XXA	B.5.5.14

The following two letters are commonly used for foreign names:

06A4	ڤ	veh	V	
06A5	پ	feh with 3 dots below	XF	

Note 1.— Not encoded.

B.5.5 Comments on Transliteration Table

B.5.5.1 Alef with madda above

Alef with madda above (آ) is not represented in the ALA-LC Romanisation Tables [1]. However, both Interpol [5] and Dr Hoogland [6] recommend the transliteration XAA.

B.5.5.2 Alef with hamza above

Alef with hamza above (أ) is not represented in the ALA-LC Romanisation Tables [1]. However, Interpol [5] recommends the transliteration XAE.

B.5.5.3 Waw with hamza above

Waw with hamza above (ؤ) is not represented in the ALA-LC Romanisation Tables [1]. U is used here as *waw with hamza above* is commonly transcribed by “U”.

B.5.5.4 Alef with hamza below

Alef with hamza below (إ) is not represented in the ALA-LC Romanisation Tables [1]. The transliteration used here is I as that Latin letter is otherwise unused, and *alef with hamza below* often commences names such as إبراهيم **(Ibrahim)** where the *alef with hamza below* is commonly transcribed by “I”.

B.5.5.5 Yeh with hamza above

Yeh with hamza above (ئ) is not represented in the ALA-LC Romanisation Tables [1]. The transliteration used here is XI as *yeh with hamza above* is used in names such as فائز **(Faiz)** where the *yeh with hamza above* is commonly transcribed by “I”.

B.5.5.6 Teh marbuta

Teh marbuta (ة) is represented in the ALA-LC Romanisation Tables [1] as H or T or TAN, depending upon the context. Dr Hoogland [6] recommends XTA. The transliteration here of *teh marbuta* has two alternatives: XTA is used generally except if *teh marbuta* occurs at the end of the name component, in which case XAH is used. This is because feminine names often use *teh marbuta* to modify a masculine name, e.g. فاطمة **(Fatimah)**. Search algorithms should take these two possibilities into account.

B.5.5.7 Hah and heh

The transliterations for *hah* (ح) and *heh* (ه) have been swapped at the advice of Interpol [5]. *Hah* is now XH and *heh* is H.

B.5.5.8 Tatwheel

Tatwheel (ـ) is a graphic character and not transliterated.

B.5.5.9 Alef maksura

Alef maksura (ى) is now transliterated as XAY at the recommendation of Dr Hoogland [6]. Other characters are transliterated as XY_, thus the former XY is incompatible.

B.5.5.10 Short vowels fatha, damma, kasra, fathatan, dammatan and kasratan

The optional short vowels (haracat) are not generally used in names and are not transliterated.

B.5.5.11 Shadda

Shadda (ّ) denotes a doubling of the consonant below it, so this is transliterated by doubling the appropriate character. Search algorithms should note that *shaddah* is optional and sometimes a doubling of the character will be present and sometimes not.

Note the special case of الله (Allah).

B.5.5.12 Sukun

Sukun (ْ) denotes the absence of a vowel, is optional, and is not transliterated.

B.5.5.13 Superscript alef

Superscript alef (ٰ) (“vowel-dagger-alef”) is not transliterated.

B.5.5.14 Alef wasla

Alef wasla (ٱ) is now transliterated as XXA at the recommendation of Interpol [5]. Other characters are transliterated XA_, thus the former XA is incompatible. Dr Hoogland [6] also recommends XXA.

B.5.6 Recommended transliteration scheme for other languages

Persian is spoken in Iran (Farsi), Afghanistan (Dari), Tajikistan and Uzbekistan.
Pashto is spoken in Afghanistan and western Pakistan.
Urdu is spoken in Pakistan and India.

Unicode	*Arabic letter*	*Language*	*Name*	*MRZ*
0679	ٹ	Urdu	tteh	XXT
067E	پ	Persian, Urdu	peh	P
067C	ټ	Pashto	teh with ring	XRT
0681	ځ	Pashto	hah with hamza above	XKE
0685	څ	Pashto	hah with 3 dots above	XXH
0686	چ	Persian, Urdu	tcheh	XC
0688	ڈ	Urdu	ddal	XXD
0689	ډ	Pashto	dal with ring	XDR
0691	ڑ	Urdu	rreh	XXR
0693	ړ	Pashto	reh with ring	XRR
0696	ږ	Pashto	reh with dot below and dot above	XRX
0698	ژ	Persian, Urdu	jeh	XJ
069A	ښ	Pashto	seen with dot below and dot above	XXS
06A9	ک	Persian, Urdu	keheh	XKK
06AB	ګ	Pashto	kaf with ring	XXK
06AD	ڭ		ng	XNG
06AF	گ	Persian, Urdu	gaf	XGG
06BA	ں	Urdu	noon ghunna	XNN
06BC	ڼ	Pashto	noon with ring	XXN
06BE	ھ	Urdu	heh doachashmee	XDO
06C0	ہ	Urdu	heh with yeh above	XYH
06C1	ہ	Urdu	heh goal	XXG
06C2	ۂ	Urdu	heh goal with hamza above	XGE
06C3	ۃ	Urdu	teh marbuta goal	XTG
06CC	ی	Persian, Urdu	farsi yeh	XYA[5]
06CD	ۍ	Pashto	yeh with tail	XXY
06D0	ې	Pashto	yeh	Y[6]
06D2	ے	Urdu	yeh barree	XYB
06D3	ۓ	Urdu	yeh barree with hamza above	XBE

[5] The letter “farsi yeh” (ی) is functionally identical to the standard “yeh” (ي) but in the isolated and final forms is graphically identical to the standard “alef maksura” (ى), so could be transliterated as ‘Y’ or “XAY”. Database matching algorithms should take this into account.
[6] The character “Pashto yeh” (ې**)** is functionally identical to the standard “yeh” (ي).

B.5.7 Example of transliteration for Standard Arabic

The example above,

ابو بكر محمد بن زكريا الرازي

can be encoded in the MRZ as:

ابو	Alef (ا) - Beh (**ب**) - Waw (**و**) => `ABW`
بكر	Beh (**ب**) – Kaf (**ك**) - Reh (ر) => `BKR`
محمد	Meem (**م**) – Hah (ح) – Meem (**م**) – Dal (**د**) => `MXHMD`
بن	Beh (**ب**) – Noon (**ن**) => `BN`
زكريا	Zain (ز) – Kaf (**ك**) – Reh (ر) – Yeh (**ي**) – Alef (ا) => `ZKRYA`
الرازي	Alef (ا) – Lam (**ل**) – Reh (ر) – Alef (ا) – Zain (ز) - Yeh (**ي**) => `ALRAZY`

i.e. `ABW<BKR<MXHMD<BN<ZKRYA<ALRAZY`

The advantages of this transliteration are:

1. The name in the Arabic script is always transliterated to the same Latin representation. This means that database matches are more likely to result;

2. The process is reversible — the name in the Arabic script can be recovered.

To recover the name in the Arabic script:

`ABW`	A=Alef (ا) - B=Beh (ب) - W=Waw (**و**) => ابو
`BKR`	B=Beh (ب) – K=Kaf (ك) - R=Reh (ر) => بكر
`MXHMD`	M=Meem (**م**) – XH=Hah (ح) – M=Meem (**م**) – D=Dal (**د**) => محمد
`BN`	B=Beh (ب) – N=Noon (ن) => بن
`ZKRYA`	Z=Zain (ز) – K=Kaf (ك) – R=Reh (ر) – Y=Yeh (ي) – A=Alef (ا) => زكريا
`ALRAZY`	A=Alef (ا) – L=Lam (ل) – R=Reh (ر) – A=Alef (ا) – Z=Zain (ز) - Y=Yeh (ي) => الرازي

The rationale for omitting the harakat and other diacritical marks is that they are optional and mostly not used. Therefore they should be treated the same way as the diacritical marks on European national characters (e.g. é, è, ç) which are used for pronunciation purposes.

As well, the optional inclusion of the harakat would be detrimental for accurate database matches.

B.5.8 Recommended transliteration scheme for Moroccan, Tunisian and Maghrib Arabic

Moroccan, Tunisian and Maghrib Arabic add four letters to the standard Arabic script:

Unicode	*Arabic letter*	*Name*	*MRZ*
069C	پ	seen with 3 dots below and 3 dots above (Moroccan)	(note 1)
06A2	ب	feh with dot moved below (Maghrib)	(note 1)
06A7	ف	qaf with dot above (Maghrib)	(note 1)
06A8	ڤ	qaf with 3 dots above (Tunisian)	(note 1)

Note 1. — These characters are obsolete and not transliterated (at the recommendation of Dr Hoogland [6]).

B.5.9 Further examples

Arabic: هاري الشماع
VIZ: **Hari Al-Schamma**
MRZ: HARY<ALXSHMAE<<<<<<<<<<<<<<<<<<<<<<<<

Arabic: سمير بادمكدوذيل
VIZ: **Samir Badmakduthal**
MRZ: SMYR<BADMKDWXDHYL<<<<<<<<<<<<<<<<<<<<<

Arabic: جمال عبد الناصر
VIZ: **Gamal Abdel Nasser**
MRZ: JMAL<EBD<ALNAXSSR<<<<<<<<<<<<<<<<<<<<<<

Arabic: العباس عبد الله بن محمد السفاح
VIZ: **al-'Abbās 'Abdu'llāh ibn Muhammad as-Saffāh**
MRZ: ALEBAS<EBD<ALLXH<BN<MXHMD<ALSFAXH<<<<<<

Arabic: عبدالله محمد بن عمر بن الحسين فخر الدين الرازي
VIZ: **Abdullah Muhammad ibn Umar ibn al-Husayn Fakhr al-Din al-Razi**
MRZ[7]: EBD<ALLXH<MXHMD<BN<EMR<BN<ALXHSYN<FXKHR

Arabic: عبدالعزيز بن متعب
VIZ: **Abdul Aziz bin Mithab**
MRZ: EBD<ALEZYZ<BN<MTEB<<<<<<<<<<<<<<<<<<<<

Arabic: إسماعيل عزّ الدين
VIZ: **Isma'il Izz-ud-din**
MRZ: ISMAEYL<EZZ<ALDYN<<<<<<<<<<<<<<<<<<<<<

Arabic: جميلة نعيمة
VIZ: **Jamillah Na'ima**
MRZ: JMYLXAH<NEYMXAH<<<<<<<<<<<<<<<<<<<<<<

[7] Truncated as specified in the form factor specific Parts 4 to 7 of Doc 9303.

B.5.10 Order of names in the MRZ

Doc 9303-3, paragraphs 4.6 and Parts 4-7, specify how primary and secondary identifiers shall be printed. This Appendix does not attempt to define primary and secondary identifiers in Arabic names. It is for the issuing authority to make that determination. But as an example:

the name in Arabic script: **ابو بكر محمد بن زكريا الرازي**

1) if the component BN<ZKRYA<ALRAZY is considered the primary identifier, then the MRZ is:

`BN<ZKRYA<ALRAZY<<ABW<BKR<MXHMD<<<<<<<<<`

2) if the component ALRAZY is considered the primary identifier, then the MRZ is:

`ALRAZY<<ABW<BKR<MXHMD<BN<ZKRYA<<<<<<<<<`

B.6 Reverse Transliteration of the MRZ

B.6.1 Table for Reverse Transliteration of the MRZ

Using the table hereunder, the Latin characters in the MRZ can be mapped back into the original Arabic script. Note that 'X' is an "escape" character and the following one or two Latin characters must be used to obtain the corresponding Arabic letter.

MRZ	*Name of Arabic letter*	*Arabic letter*	*Unicode*
A	alef	ا	0627
B	beh	ب	0628
D	dal	د	062F
E	ain	ع	0639
F	feh	ف	0641
G	ghain	غ	063A
H	heh	ه	0647
I	alef with hamza below	إ	0625
J	jeem	ج	062C
K	kaf	ك	0643
L	lam	ل	0644
M	meem	م	0645
N	noon	ن	0646
P	peh (Persian, Urdu)	پ	067E
Q	qaf	ق	0642
R	reh	ر	0631
S	seen	س	0633
T	teh	ت	062A
U	waw with hamza above	ؤ	0624
V	veh	ڤ	06A4
W	waw	و	0648
Y	yeh or yeh (Pashto)	ي / ې	064A/06D0
Z	zain	ز	0632

MRZ	Name of Arabic letter	Arabic letter	Unicode
XAA	alef with madda above	آ	0622
XAE	alef with hamza above	أ	0623
XAH	teh marbuta (see also xta)	ة	0629
XAY	alef maksura	ى	0649
XBE	yeh barree with hamza above	ۓ	06D3
XC	tcheh (Persian, Urdu)	چ	0686
XDH	thal	ذ	0630
XDO	heh doachashmee	ھ	06BE
XDR	dal with ring (Pashto)	ډ	0689
XDZ	dad	ض	0636
XE	hamza	ء	0621
XF	feh with 3 dots below	ڟ	06A5
XGG	gaf (Persian, Urdu)	گ	06AF
XGE	heh goal with hamza above (Urdu)	ۂ	06C2
XH	hah	ح	062D
XI	yeh with hamza above	ئ	0626
XJ	jeh (Urdu)	ژ	0698
XKE	hah with hamza above (Pashto)	ځ	0681
XKH	khah	خ	062E
XKK	keheh (Persian, Urdu)	ک	06A9
XNN	noon ghunna (Urdu)	ں	06BA
XNG	ng	ڭ	06AD
XRR	reh with ring (Pashto)	ړ	0693
XRT	teh with ring	ټ	067C
XRX	reh with dot below and dot above (Pashto)	ږ	0696
XSH	sheen	ش	0634
XSS	sad	ص	0635
XTA	teh marbuta (see also XAH)	ة	0629
XTG	teh marbuta goal (Urdu)	ۃ	06C3
XTH	theh	ث	062B
XTT	tah	ط	0637
XXA	alef wasla	ٱ	0671
XXD	ddal (Urdu)	ڈ	0688
XXG	heh goal (Urdu)	ہ	06C1
XXH	hah with 3 dots above (Pashto)	څ	0685
XXK	kaf with ring (Pashto)	ګ	06AB
XXN	noon with ring (Pashto)	ڼ	06BC
XXR	rreh (Urdu)	ڑ	0691
XXS	seen with dot below and dot above (Pashto)	ښ	069A
XXT	tteh (Urdu)	ٹ	0679
XXY	yeh with tail (Pashto)	ۍ	06CD
XYA	farsi yeh (Persian, Urdu)	ی	06CC
XYB	yeh barree (Urdu)	ے	06D2
XYH	heh with yeh above (Urdu)	ۀ	06C0
XZZ	zah	ظ	0638

B.7 Computer Programs

B.7.1 Arabic to MRZ

This program written in Python is offered as an example of converting Arabic characters (in Unicode) to the MRZ format.

The Arabic characters are contained in a file “Arabic source.txt” and the corresponding MRZ data is written to a file “MRZ output.txt”.

****

```
#    # -*- coding: iso-8859-15 -*-

import unicodedata
import encodings.utf_8_sig
import codecs

# TRANSLITERATE
def Arabic_to_MRZ(unicode_string):
   transform = {0x20: '<', 0x21: 'XE', 0x22: 'XAA', 0x23: 'XAE', 0x24: 'U',
               0x25: 'I', 0x26: 'XI', 0x27: 'A', 0x28: 'B', 0x29: 'XAH',
               0x2A: 'T', 0x2B: 'XTH', 0x2C: 'J', 0x2D: 'XH', 0x2E: 'XKH',
               0x2F: 'D', 0x30: 'XDH', 0x31: 'R', 0x32: 'Z', 0x33: 'S', 0x34: 'XSH',
               0x35: 'XSS', 0x36: 'XDZ', 0x37: 'XTT', 0x38: 'XZZ', 0x39: 'E',
               0x3A: 'G', 0x41: 'F', 0x42: 'Q', 0x43: 'K', 0x44: 'L',
               0x45: 'M', 0x46: 'N', 0x47: 'H', 0x48: 'W', 0x49: 'XAY',
               0x4A: 'Y', 0x71: 'XXA', 0x79: 'XXT', 0x7E: 'P', 0x7C: 'XRT',
               0x81: 'XKE', 0x85: 'XXH', 0x86: 'XC', 0x88: 'XXD', 0x89: 'XDR',
               0x91: 'XXR', 0x93: 'XRR', 0x96: 'XRX', 0x98: 'XJ', 0x9A: 'XXS',
               0xA4: 'XV', 0xA5: 'XF', 0xA9: 'XKK', 0xAB: 'XXK', 0xAD: 'XNG',
               0xAF: 'XGG', 0xBA: 'XNN', 0xBC: 'XXN', 0xBE: 'XDO', 0xC0: 'XYH',
               0xC1: 'XXG', 0xC2: 'XGE', 0xC3: 'XTG',
               0xCC: 'XYA', 0xCD: 'XXY', 0xD0: 'Y', 0xD2: 'XYB', 0xD3: 'XBE'}
   name_in = unicode_string
   name_out = ""
   for c in name_in:
# check for shadda (double)
      if ord(c) == 0x51:
         name_out = name_out + char
      else:
         if ord(c) in transform:
            char = transform[ord(c)]
            name_out = name_out + char
   print name_out
   return name_out

#
#   MAIN - Arabic to MRZ
#

# open input and output files
```

```
fin = encodings.utf_8_sig.codecs.open('Arabic source.txt', 'r') #b', 'utf-8-sig', 'ignore', 1)
fout = open('MRZ output.txt', 'w')

# loop through the input file

try:
    for arabic_name in fin:
        MRZ_name = Arabic_to_MRZ(arabic_name)
        fout.write(MRZ_name)
        fout.write('\n')
finally:
    fin.close()
fout.flush()
fout.close()
```

****

B.7.2 MRZ to Arabic

This program written in Python is offered as an example of converting MRZ characters to Arabic characters (in Unicode).

The MRZ characters are contained in a file “MRZ source.txt” and the corresponding Arabic data is written to a file “Arabic output.txt”.

****

```
#    # -*- coding: iso-8859-15 -*-

import unicodedata
import encodings.utf_8_sig
import codecs

# TRANSLITERATE
def MRZ_to_Arabic(ascii_string):
    transform = { '<': 0x20, 'XE': 0x21, 'XAA':0x22, 'XAE': 0x23, 'U': 0x24,
                  'I': 0x25, 'XI': 0x26, 'A': 0x27, 'B': 0x28, 'XAH': 0x29,
                  'T': 0x2A, 'XTH': 0x2B, 'J': 0x2C, 'XH': 0x2D, 'XKH': 0x2E,
                  'D': 0x2F, 'XDH': 0x30, 'R': 0x31, 'Z': 0x32, 'S': 0x33, 'XSH': 0x34,
                  'XSS': 0x35, 'XDZ': 0x36, 'XTT': 0x37, 'XZZ': 0x38, 'E': 0x39,
                  'G': 0x3A, 'F': 0x41, 'Q': 0x42, 'K': 0x43, 'L': 0x44, 'M': 0x45,
                  'N': 0x46, 'H': 0x47, 'W': 0x48, 'XAY': 0x49, 'Y': 0x4A, 'XXA': 0x71,
                  'XXT': 0x79, 'P': 0x7E, 'XRT': 0x7C, 'XKE': 0x81, 'XXH': 0x85,
                  'XC': 0x86, 'XXD': 0x88, 'XDR': 0x89, 'XXR': 0x91, 'XRR': 0x93,
                  'XRX': 0x96, 'XJ': 0x98, 'XXS': 0x9A, 'XV': 0xA4, 'XF': 0xA5,
                  'XKK': 0xA9, 'XXK': 0xAB, 'XNG': 0xAD, 'XGG': 0xAF,
                  'XNN': 0xBA, 'XXN': 0xBC, 'XDO': 0xBE, 'XYH': 0xC0,
                  'XXG': 0xC1, 'XGE': 0xC2, ‘XTA’: 0x29, 'XTG': 0xC3, 'XYA': 0xCC,
                  'XXY': 0xCD, 'I': 0xD0, 'XYB': 0xD2, 'XBE': 0xD3}
    name_in = ascii_string
```

```
    name_out = ""
    # if this character is not X, does it appear by itself in the table?
    search_string = ''
    last_string = ''
    iloop = 0
    while iloop < len(name_in):
        search_string = search_string + name_in[iloop]
        if search_string in transform:
            if search_string <> last_string:
                name_out = name_out + chr((transform[search_string]))
            #insert shadda if double found
            else:
                name_out = name_out + chr(0x51)
            if search_string <> '<':
                name_out = name_out + chr(0x06)
            else:
                name_out = name_out + chr(0x00)
            #remember last string
            if search_string <> '<':
                last_string = search_string
            else:
                last_string = ''
            #clear the search string once found
            search_string = ''
        iloop = iloop + 1
    print name_out
    return name_out

#
#   MAIN - MRZ to Arabic
#

# open input and output files

fin = open('MRZ source.txt', 'r')
fout = open('Arabic output.txt', 'wb') #b', 'utf-8-sig', 'strict', 1)
fout.write(encodings.utf_8_sig.codecs.BOM)


# loop through the input file

try:
    for MRZ_name in fin:
        Arabic_name = MRZ_to_Arabic(MRZ_name)
        Arabic_name = Arabic_name + chr(0x0D) + chr(0x00) + chr(0x0A) + chr(0x00)
        fout.write(Arabic_name)
finally:
    fin.close()
fout.flush()
fout.close()

*****************************************************************************
```

B.8 References (Informative)

[1] *ALA-LC Romanization Tables: Transliteration Schemes for Non-Roman Scripts.* Randal K. Berry (ed.). Library of Congress, 1997.

[2] *The Encyclopedia of Islam*. New Edition. Leiden, 1960.

[3] *ISO 233:1984. Documentation - Transliteration of Arabic characters into Latin characters*. International Organization for Standardization, 1984-12-15.

[4] *United Nations Romanization Systems for Geographical Names. Report on Their Current Status*. Compiled by the UNGEGN Working Group on Romanization Systems. Version 2.1. June 2002.

[5] *IPSG comments to the document: Transliteration of Arabic Fonts in Machine Readable Travel Documents - Technical Report - Version 2.3 dated 15 Feb 2008*. Interpol, Lyon, 17 March 2008.

[6] Private correspondence, Dr. Jan Hoogland, Department of Arabic, University of Nijmegen, the Netherlands, 23 March 2008.

[7] *Comments on the Translation of Arabic Fonts in Machine Readable Travel Documents TECHNICAL REPORT AMA 13052008*, Mr. Abdalla M. Askar, Emirates Identity Authority.

—END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 20XX

Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 4 — *Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs*
ISBN 978-92-9249-793-4

DOCUMENT CHANGE RECORD

Doc 9303, Part 4

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

1. SCOPE

Doc 9303, Part 4 defines specifications that are specific to TD3 size Machine Readable Passports (MRPs) and other TD3 size Machine Readable Travel Documents (MRTDs). For brevity the term MRP has been used throughout this document and, except where stated, all the specifications herein shall apply equally to all other TD3 size MRTDs. This document shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*;
- Part 3 — *Specifications Common to all MRTDs*.

Together these specifications provide for global data interchange of MRTDs both by visual (eye readable) and machine readable (optical character recognition) means.

Additional specifications providing for global data interchange of electronic data in eMRPs and eMROTDs can be found in Doc 9303, Parts 9 through 12.

2. CONSTRUCTION AND DIMENSIONS OF THE MRP AND MRP DATA PAGE

2.1 Construction

The MRP shall take the form of a book consisting of a cover and a minimum of eight pages and shall include a data page onto which the issuing State or organization enters the personal data relating to the holder of the document and data concerning the issuance and validity of the MRP. After issuance no additional pages shall be added to the MRP.

2.2 MRP Data Page Nominal Dimensions

The nominal dimensions shall be as specified in ISO/IEC 7810: 2019 (except thickness) for the TD3 size MRTD, i.e.:

125.00 mm (4.921 in) wide by 88.00 mm (3.465 in) high

2.3 MRP Data Page Edge Tolerances

The edges of the data page following final preparation shall be within the area circumscribed by the concentric rectangles as illustrated in Figure 1.

Inner rectangle: 87.25 mm × 124.25 mm (3.44 in × 4.89 in)
Outer rectangle: 88.75 mm × 125.75 mm (3.49 in × 4.95 in)

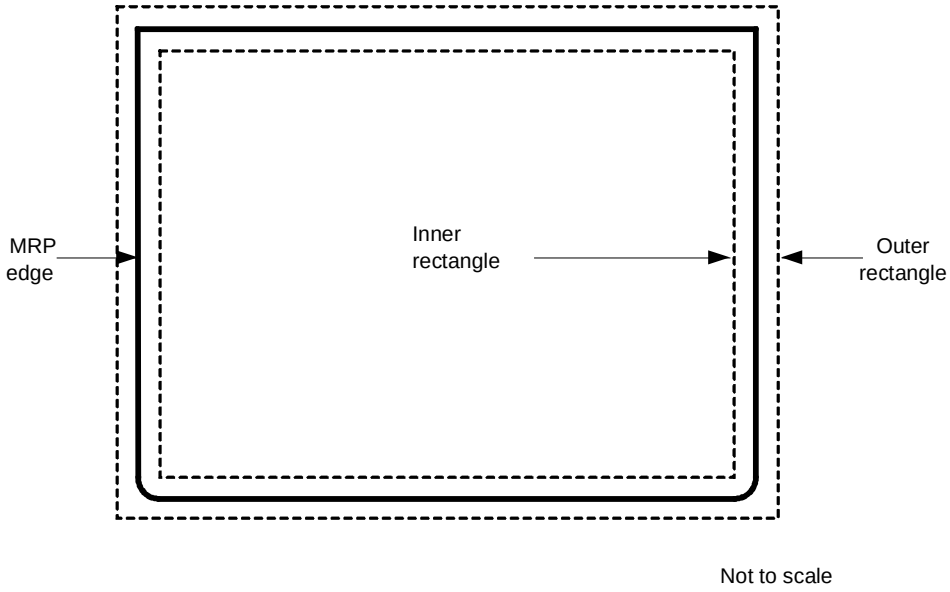


Figure 1. MRP data page dimensional illustration

2.4 MRP Data Page Margins

The dimensional specifications refer to the outer limits of the MRP data page. A margin of 2.0 mm (0.08 in) along the left and right hand edges and top edge must be left clear of data, as shown in Figure 2. The position of data in the machine readable zone is as shown in Figure 3.

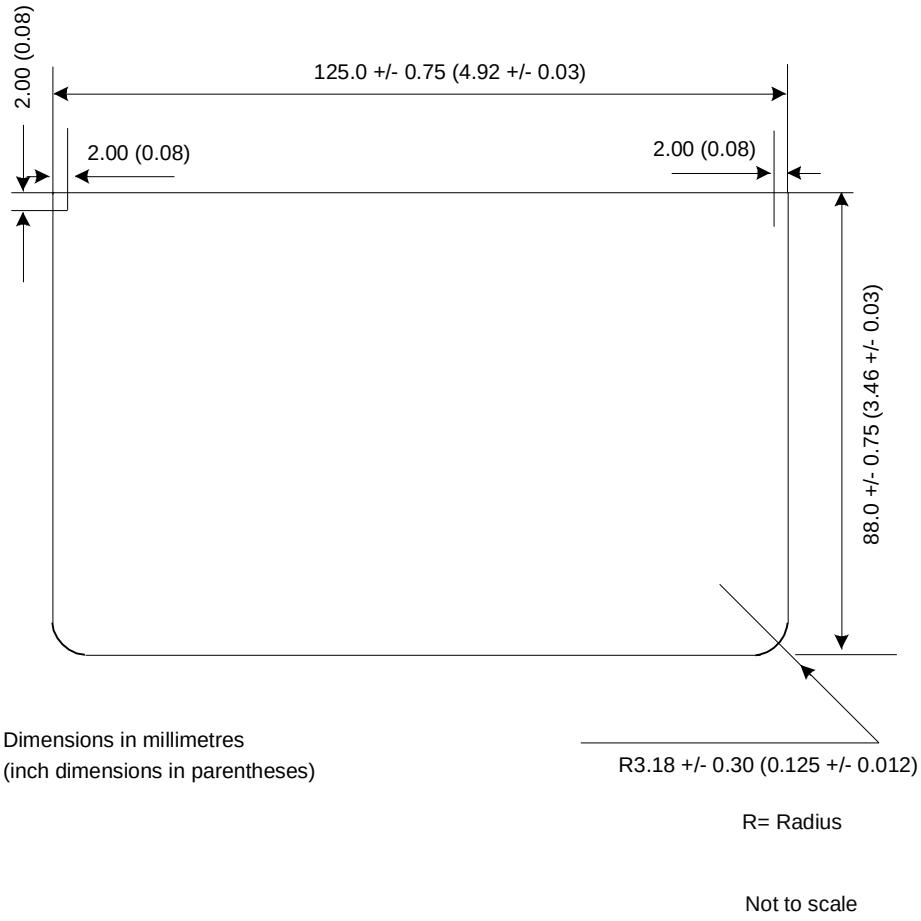


Figure 2. Edge margins of the MRP data page

2.5 MRP Data Page Thickness

The thickness, including any final preparation (e.g. laminate), shall be as follows:

- Minimum:

No minimum thickness is specified. However, States are advised that currently available materials are unlikely to provide an adequately robust data page if the thickness is below 0.15 mm (0.006 in);

- Maximum:

0.90 mm (0.035 in).

The thickness of the area within the machine readable zone shall not vary by more than 0.10 mm (0.004 in).

General note.— The decimal notation in these specifications conforms to ICAO practice. This differs from the ISO practice, which is to use a decimal point (.) in imperial measurements and a comma (,) in metric measurements.

2.6 MRP Dimensions

The dimensional specifications defined in Paragraphs 2.2 to 2.3 above also apply to the MRP book. If required for binding purposes, the 88.0 mm (3.46 in) dimension may be increased.

The 88.0 mm (3.46 in) dimension associated with polycarbonate data pages (or equivalent) includes any hinge material as measured from the bottom of the data page to the stitching line.

3. GENERAL LAYOUT OF THE MRP DATA PAGE

The MRP data page follows a standardized layout to facilitate reading of data globally by visual and machine readable means.

The MRP data page should either be an inner page in close proximity to an end leaf of the MRP or form part of the cover of the MRP. Where the MRP data page is part of the cover, precautions must be taken to ensure that the endleaf/cover assembly combined with the means of personalization are together resistant to fraudulent attack, particularly by delamination of the cover structure. Where the MRP data page is not constructed as part of the cover, the recommended practice is to locate the MRP data page on page 2 or on the penultimate page of the MRP. The location of the MRP data page in any other position in the MRP will give rise to problems for document examiners in the operation of swipe readers reading the MRZ. The MRZ shall be positioned adjacent to the outside long edge of the book, parallel to the spine of the book (see Figures 3 and 4).

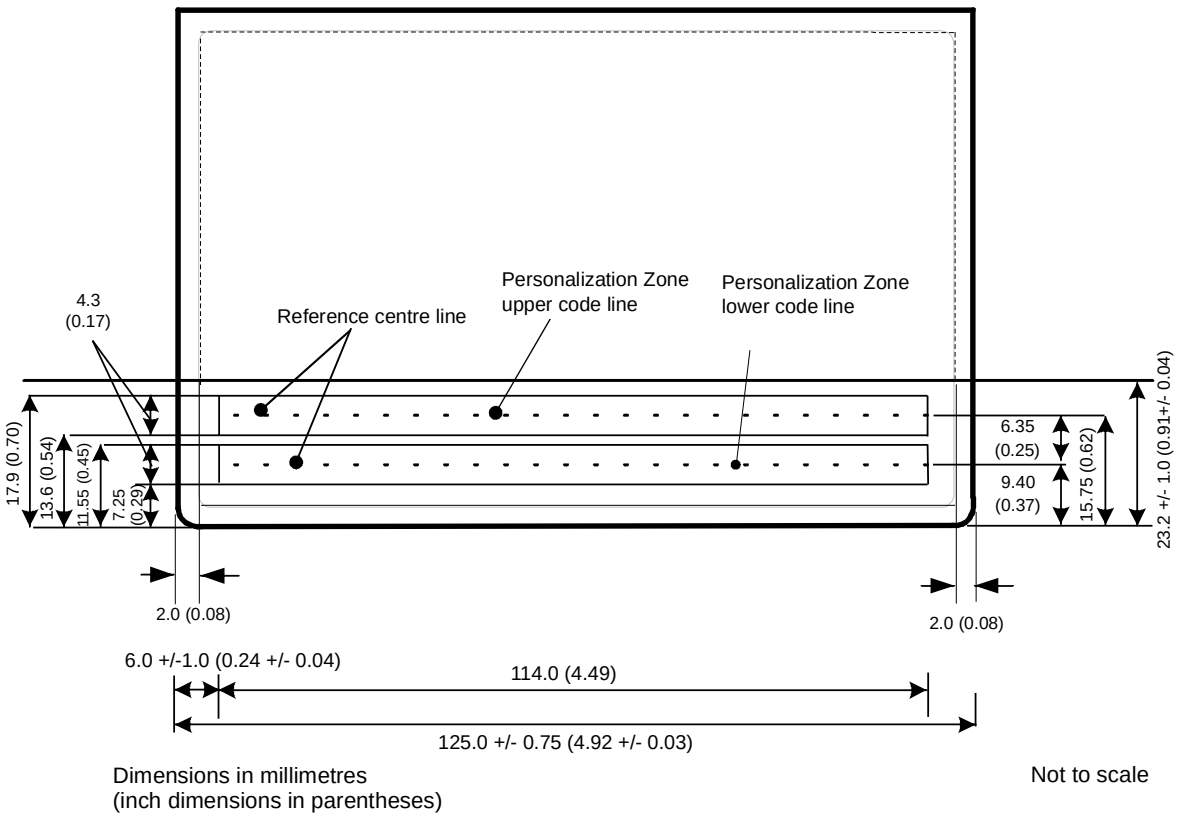


Figure 3. Schematic diagram of the Machine Readable Zone (MRZ)

3.1 MRP Zones

To accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements, the MRP data page is divided into seven zones as follows:

3.1.1 Front of MRP data page

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Mandatory holder's signature or usual mark (original or reproduction)
Zone V	Mandatory identification feature
Zone VII	Mandatory machine readable zone (MRZ)

3.1.2 Back of MRP data page, or an adjacent page

Zone VI	Optional data elements

3.2 Content and Use of Zones

Zones I to V, which, together with Zone VI, form the Visual Inspection Zone (VIZ), and Zone VII, which is the Machine Readable Zone (MRZ), contain mandatory elements in a standard sequence which represent the minimum requirements for the MRP data page. The optional elements in Zones II, III and VI accommodate the diverse requirements of issuing States or organizations, allowing for presentation of additional data at the discretion of the issuing State or organization, while achieving the desired level of standardization. The location of zones and standard sequence for data elements are set out in Figure 4. The technical specifications for the printing of data on the MRP data page are defined in Section 4. Figures 8, 9 and 10 outline the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States or organizations. Some examples of personalized MRP data pages are shown in Appendix A.

3.2.1 Zone IV — Location of holder's signature or usual mark

Field 18, the holder's signature or usual mark (or a reproduction thereof), shall normally be placed in Zone IV of the MRP data page (see Figure 4). Where the issuing State or organization wishes to locate the holder's signature or usual mark on a page other than the MRP data page, it may, as specified in the Data Element Directory, relocate Field 18 to Zone VI on the back of the MRP data page or to the page adjacent to the MRP data page. In this case, the size of adjacent fields in the visual zone on the MRP data page may be increased.

3.2.2 Zone V — Position of holder's portrait

Within Zone V, the holder's portrait shall be at least 2.0 mm (0.08 in) from the left-hand edge of the MRP data page. The use of affixed or stick-on portrait photos is not permitted and these shall not be used. Instead, the portrait image shall be integrated with the biodata page using a secure personalization technology.

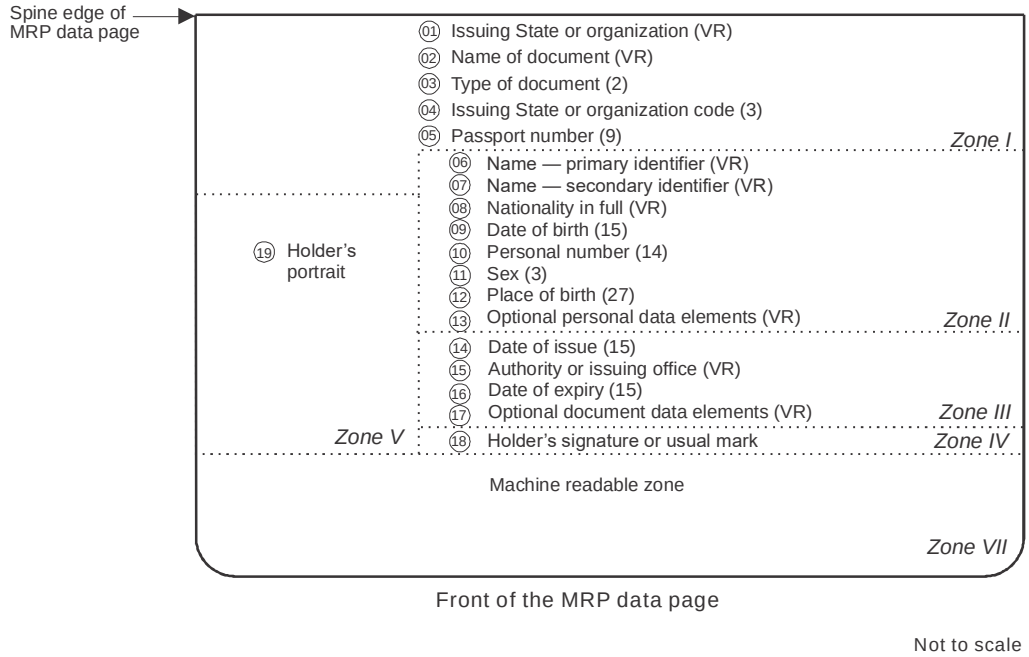


Figure 4. Sequence of data elements on front side of MRP data page

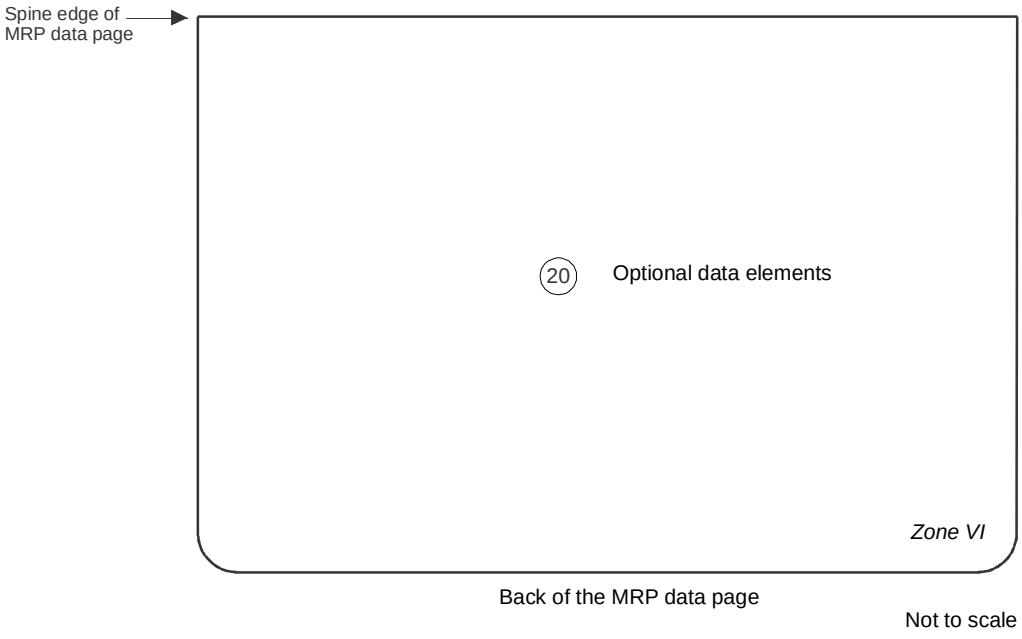


Figure 5. Data elements on reverse side

Notes to Figures 4 and 5:
Note 1.— (VR) = variable number of characters in field.
Note 2.— (n) = the maximum or fixed number of characters allowed in the field.
Note 3.— O = indicates the field number.

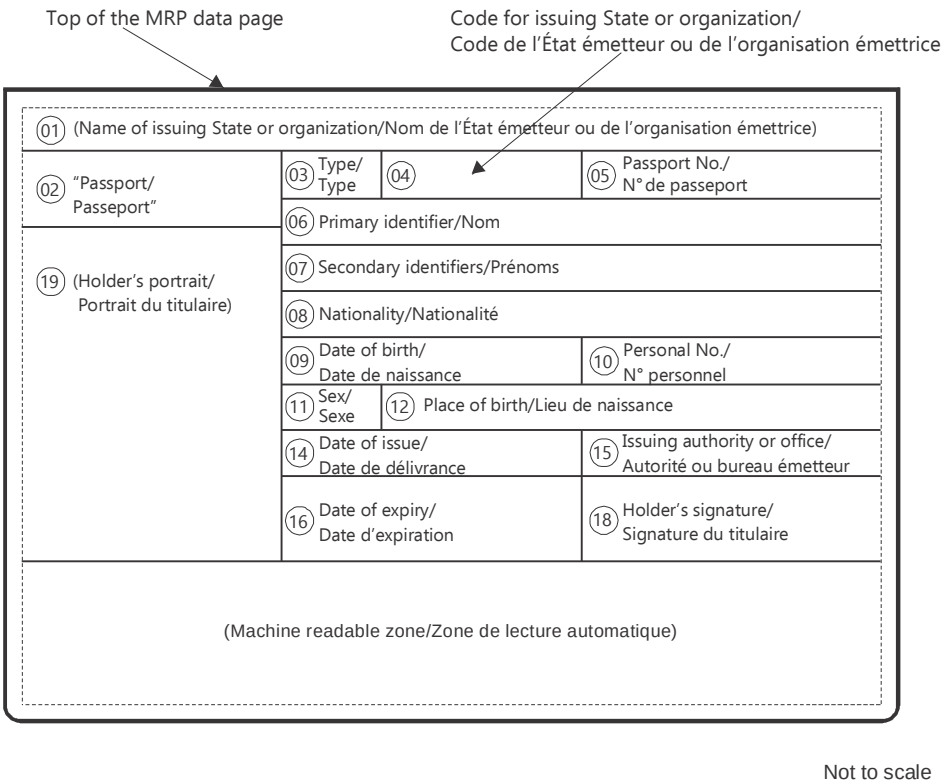
3.2.3 Data elements

The data elements to be included in the zones, the preparation of the zones and guidelines for the dimensional layout of zones shall be as described in Section 4 of this Part.

3.2.4 Mandatory zones

The MRP data page shall contain Zones I, II, III, V and VII. If the issuing State or organization's practice is to omit mandatory elements 01 and 02 (issuing State or organization, in full, and document, in full) from the header (Zone I), these data elements shall be placed on an adjacent or preceding page.

Zone IV shall be present either on the data page or on an adjacent page and contain the holder's signature or usual mark, i.e. original or reproduction. Alternatively, at the discretion of the issuing State or organization, the holder's signature may be located in Zone VI on the reverse side of the MRP data page. Zone V shall include the personal identification feature(s) which shall include a portrait solely of the rightful holder. At the discretion of the issuing State or organization, the name fields in Zone II and the holder's signature or usual mark in Zone IV may overlay Zone V provided this does not hinder recognition of the data in any of the three zones.



Note 1.— Optional data Fields 13 and 17 are excluded in the recommended practice.
Note 2.— Captions corresponding to the field names printed in the above illustration, except those within parentheses, shall be printed on the MRP data page.

Figure 6. Schematic of nominal layout of data elements

Data elements shall appear in a standard sequence as shown in Figures 4 and 5. Figure 6 is a schematic of the nominal layout of data elements on the front side of an MRP data page, and Figure 7 is a template for the position of the personalized data fields.

The dimensions and boundaries of Zone VII, the machine readable zone, are fixed. Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the effective reading zone (ERZ) specified in Doc 9303-3.

MRZ (Zone VII) data elements shall be as defined in Paragraph 4.2.2 and illustrated in Appendix B, Figure 15.

3.2.5 Optional data zone

Zone VI, which may be on the back of the data page or on an adjacent page, is a zone for optional data for use at the discretion of the issuing State or organization.

A template for the layout of personalized data elements on the front side of an MRP data page is shown in Figure 7.

3.3 Dimensional Flexibility of Zones I to V

Zones I to V may be adjusted in size and shape within the overall dimensional specifications of the MRP data page to accommodate the diverse requirements of issuing States or organizations. All zones, however, shall be bounded by straight lines, and all angles where straight lines join shall be right angles (i.e. 90 degrees). It is recommended that the zone boundaries not be printed on the MRP data page. The nominal position of the zones is shown in Figure 8.

When an issuing State or organization chooses to produce an MRP data page that contains a transparent or otherwise unprintable border, this will result in a reduction of the available area within the zones. The full MRP data page dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the MRP data page.

Zone I shall be located along the top edge of the MRP data page and extend across the full 125.0 ± 0.75 mm (4.92 ± 0.03 in) dimension. (The top edge is the edge coincident with the spine of the MRP.) The issuing State or organization may vary the *vertical* dimension of Zone I, as required, but this dimension shall be sufficient to allow legible interpretation of the data elements in the zone and shall not be greater than 17.9 mm (0.70 in).

Zone V shall be located such that its left edge is coincident with the left edge of the MRP data page as shown in Figure 8. The dimensions of the portrait contained in Zone V are specified in Section 4.1.1.1, the Visual Data Element Directory, Field 19.

Zone V may move *vertically* along the left edge of the MRP data page and overlay a portion of Zone I as long as individual details contained in either zone are not obscured.

The upper boundary of Zone II shall be coincident with the lower boundary of Zone I.

When there is a specific requirement for the name fields to extend across the MRP data page, Zone II may extend up to the full 125.0 ± 0.75 mm (4.92 ± 0.03 in) dimension of the MRP data page. If the full dimension is used, Zone II shall overlay a portion of Zone V. In this case, issuing States or organizations shall ensure that data contained in either zone is not obscured.

The lower boundary of Zone II may be positioned at the discretion of the issuing State or organization. Enough space must be left for Zones III and IV below the boundary. This boundary does not need to be straight across the 125.0 ± 0.75 mm (4.92 ± 0.03 in) dimension of the MRP data page. This is illustrated in Figure 9.

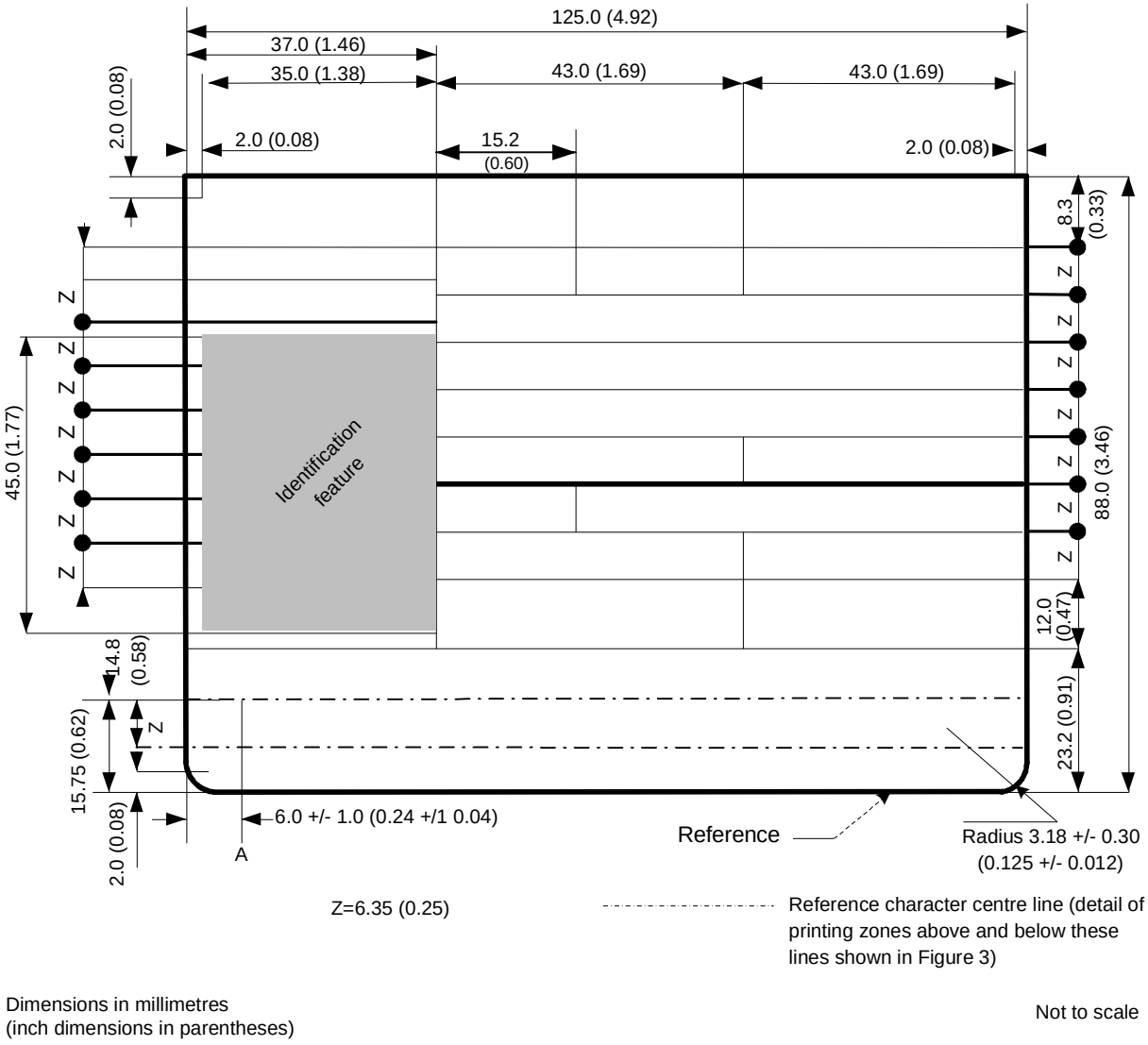


Figure 7. Template for the personalization data fields

Note 1.— To allow for variations during manufacture of the MRP, a tolerance of ± 1.0 mm (± 0.04 in) is allowed for the 23.2 mm (0.91 in) dimension of the MRZ and within that overall tolerance the boundary between the VIZ and the MRZ shall not be skewed more than 0.5 mm (0.02 in) over the 125.0 mm (4.92 in) dimension.

Note 2.— 'A' — There shall be no text to the left of this line in the MRZ.

Note 3.— Except for background security print there shall be no print in the 2.0 mm (0.08 in) margins.

Note 4.— The borderlines of the fields shall be omitted on the actual MRP data page.

Note 5 – When the printed photograph occupies the maximum area of 35mm x 45mm within Zone V, an additional horizontal tolerance up to 2mm is allowable.

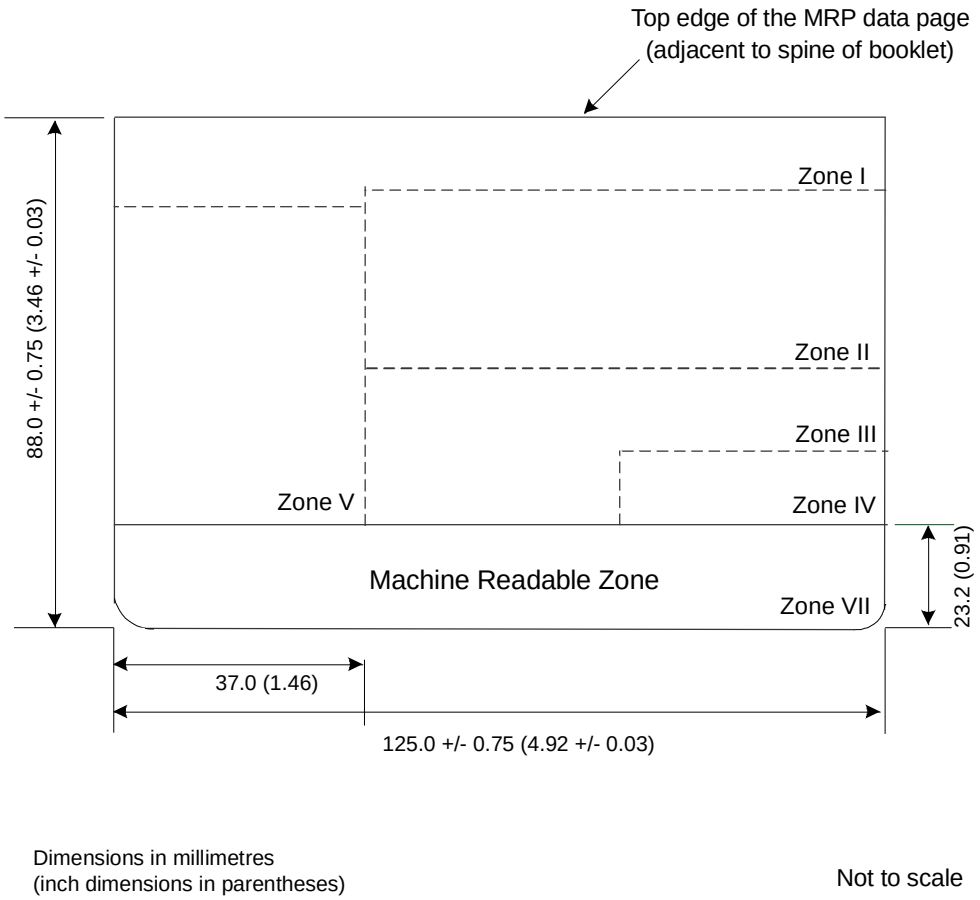


Figure 8. Nominal positions of Zones I-V

Note 1.— Dotted lines indicate zone boundaries whose positions are not fixed, enabling issuing States or organizations flexibility in the presentation of data. See paragraph 3.3.

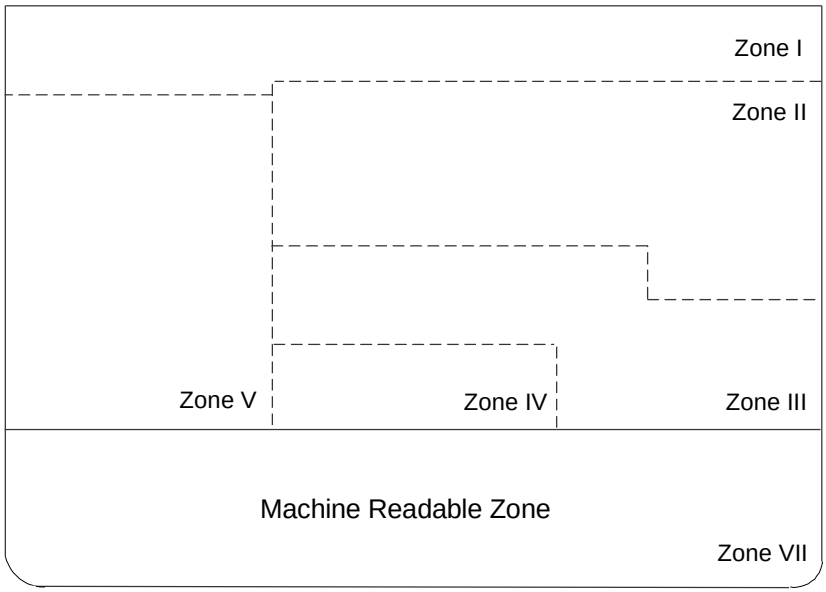
Note 2.— Zone VI, where used, appears on the back of the data page or on an adjacent page.

Zone III should start at the right vertical boundary of Zone V and may extend, at the discretion of the issuing State or organization, to the right edge of the MRP data page. Figures 9 and 10 illustrate the flexibility permitted to issuing States or organizations.

If Zone IV is placed on the MRP data page, it shall be at the bottom of the VIZ on the front of the MRP data page, its lower boundary coincident with the top edge of the MRZ. Figures 8 and 9 show two alternative positions for Zone IV. Figure 10 shows an MRP data page where Zone IV has been placed on an adjacent page.

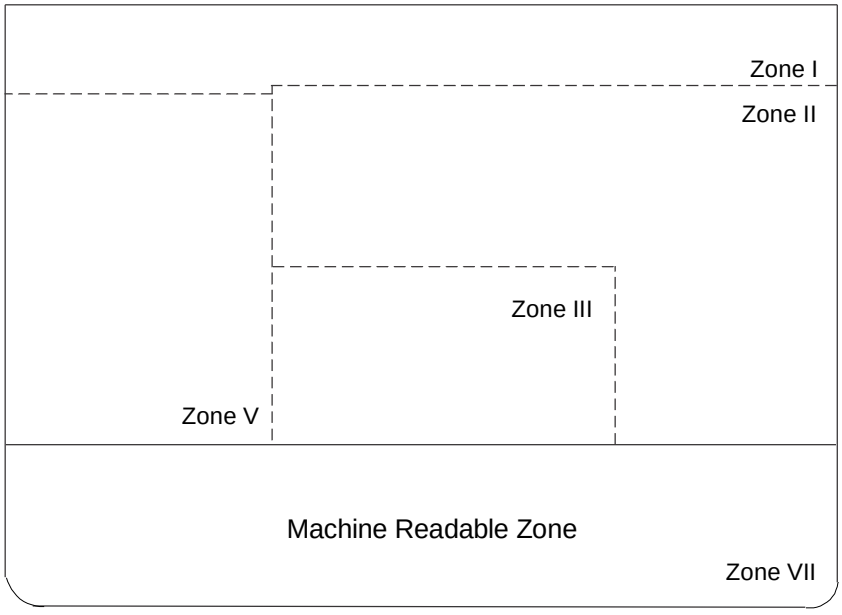
Zone IV may also overlay Zone V, though this practice is not recommended. In this case, issuing States or organizations shall ensure that individual details contained in either zone are not obscured. See Appendix A, Figure 13.

When an issuing State or organization wishes to have a displayed image of an MRP holder’s fingerprint, the image may be displayed within the area designated for Zone II as illustrated in Appendix A, Figure 14.



Not to scale

Figure 9. Example of flexible positioning of zones illustrating a staircase boundary between Zones II and III



Not to scale

Figure 10. Example of flexible positioning of zones in which Zone IV (signature) is moved to an adjacent page and Zone III positioned such that it does not extend to the right-hand edge of the data page

4. CONTENTS OF THE MRP DATA PAGE

4.1 Visual Inspection Zone (VIZ) (Zones I through VI)

Guidance on the typeface, size and line spacing, the languages and character set, to be used in the VIZ may be found in Doc 9303-3.

If any optional field or data element is not used, the data may be spread more evenly in the visual zone of the MRP data page consistent with the requirement for sequencing zones and data elements.

4.1.1 Data element directory

The data elements in the VIZ are specified as follows**:**

4.1.1.1 Visual inspection zone — Data element directory

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
01/I (Mandatory)	Issuing State or organization (in full)	The name of the State or organization responsible for issuing the MRP shall be displayed in full. For additional details see Doc 9303-3.	Variable	Notes a, c, d, f, g. If omitted, shall appear on an adjacent or preceding page in the passport.
02/I (Mandatory)	Document	The word for “passport” in the language of the issuing State or organization, plus either PASSPORT (English), PASSEPORT (French) or PASAPORTE (Spanish) if the language of the issuing State or organization is not English, French or Spanish. For additional details see Doc 9303-3.	Variable	Notes a, c, d, g, m, n. If omitted, shall appear on an adjacent or preceding page in the passport.
03/I (Mandatory)	Document code	Capital letter P to designate an MRP. One additional capital letter may be used, in the character position after the letter P and at the discretion of the issuing State or organization, to designate other types of passports such as MRP issued to diplomatic staff,	2	Notes a, g, l, m.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
		an MRP issued for travel on government business, or a passport issued for a special purpose.		
04/I (Mandatory)	Issuing State or organization (in code)	As abbreviated in the three-letter code specified in Doc 9303-3.	3 Fixed	Notes a, f, l.
05/I (Mandatory)	Passport Number	As given by the issuing State or organization to uniquely identify the document from all other MRTDs issued by the State or organization. For additional details see Doc 9303-3.	9	Notes a, b, c, g, l.
06/07/II (Mandatory)	Name	The full name of the holder, as identified by the issuing State or organization. For additional details see Doc 9303-3.	Variable	Notes a, c, g, k, l.
06/II (Mandatory)	Primary Identifier	Predominant component(s) of the name of the holder as described in Doc 9303-3. In cases where the predominant component(s) of the name of the holder (e.g. where this consists of composite names) cannot be shown in full or in the same order, owing to space limitations of Field(s) 06 and/or 07 or national practice, the most important component(s) (as determined by the State or organization) of the primary identifier shall be inserted.	Variable	Notes a, c, g, k, l.
07/II (Mandatory)	Secondary Identifier	Secondary component(s) of the name of the holder as described in Doc 9303-3. The most important component(s) (as determined by the State or organization) of the secondary identifier of the holder shall be inserted in full, up to the maximum dimensions of the field frame. Other components, where necessary, may be	Variable	Notes a, c, k, g, l.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
		represented by initials. Where the holder's name has only predominant component(s), this data field shall be left blank. A State may optionally utilize the whole zone comprising Fields 06 and 07 as a single field. In such a case, the primary identifier shall be placed first, followed by a comma and a space, followed by the secondary identifier.		
08/II (Mandatory)	Nationality	For details see Doc 9303-3.	Variable	Notes a, c, f, g, l, o.
09/II (Mandatory)	Date of birth	Holder's date of birth as recorded by the issuing State or organization. If the date of birth is unknown, see Doc 9303-3 for guidance.	Variable	Notes a, b, c, g, l.
10/II (Optional)	Personal number	Field optionally used for personal identification number given to holder by the issuing State or organization. For additional details see Doc 9303-3.	Variable	Notes a, b, c, e, g.
11/II (Mandatory)	Sex	Sex of the holder, to be specified by use of the single initial commonly used in the language of the State or organization where the document is issued and, if translation into English, French or Spanish is necessary, followed by an oblique and the capital letter F for female, M for male, or X for unspecified.	3	Notes a, c, g, l, p.
12/II (Optional element in mandatory zone)	Place of birth	Field optionally used for city and State of the holder's birthplace. Refer to Doc 9303-3 for further details.	Variable	Notes a, c, e, f, g.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
13/II (Optional element in mandatory zone)	Optional personal data elements	Optional personal data elements e.g. personal identification number or fingerprint, at the discretion of the issuing State or organization. If a fingerprint is included in this field, it should be presented as a 1:1 representation of the original. If a date is included it shall follow the form of presentation described in Doc 9303-3.	Variable	Notes a, b, c, e, g, i.
14/III (Mandatory)	Date of issue	For details see Doc 9303-3.	Variable	Notes a, b, c, g, i, l.
15/III (Mandatory)	Authority or issuing organization	Authority or issuing organization for the MRP. This field shall be used to indicate the issuing authority or issuing organization and, optionally, its location, which may be personalized within this field. For additional details see Doc 9303-3.	Variable	Notes a, b, c, f, g, j, l.
16/III (Mandatory)	Date of expiry	Date of expiry of the MRP. For additional details see Doc 9303-3.	Variable	Notes a, b, c, g, l.
17/III Optional element in mandatory zone	Optional document data elements	Optional data elements relating to the document. For additional details see Doc 9303-3.	Variable	Notes a, b, c, e, g.
18/IV (Mandatory)	Holder’s signature or usual mark	At the discretion of the issuing State or organization, the signature or usual mark may be located in Zone VI. The size of the field to be allocated to the signature or usual mark on the adjoining page shall be at the discretion of the issuing State or organization, subject to the overall dimensional limits of the MRP. For additional details see Doc 9303-3.	Variable	Notes e, j.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
19/V (Mandatory)	Identification feature	This field shall contain a portrait of the holder. The portrait shall not be larger than 45.0 mm x 35.0 mm (1.77 in x 1.38 in) nor smaller than 32.0 mm x 26.0 mm (1.26 in x 1.02 in). The position of the field concerned shall be aligned to the left of Zones II, III and IV. See Doc 9303-3 for additional specifications for the portrait.		Note d.
20/VI (Optional)	Optional data elements	Additional optional data elements at the discretion of the issuing State or organization. For additional details see Doc 9303-3.		Notes a, b, c, e, g, i.

** Notes can be found in the last portion of sub-section 4.2.2.2.*

4.1.1.2 Card access number

For MRPs containing a contactless IC, issuing States or organizations may, at their discretion, wish to include a Card Access Number (CAN) on the datapage or the page adjacent to the datapage to facilitate machine reading and data capture from the chip.

Specifically, the purpose of the CAN is to enable the chip to be accessed without reading the MRZ. When the chip supports PACE, this can be accomplished by adding a CAN. The CAN and its position within the MRP are specified as follows.

The CAN is a 6-digit number, comprised solely of numerals, 0 to 9. There is no check digit since the check is implicitly performed by the protocol. The CAN should include a field caption.

Recognizing that the issuing State or organizations have diverse requirements for the layout of the VIZ, the CAN shall appear on either the data page or the page adjacent to the data page, and should appear in the VIZ. The horizontal and vertical position shall be at the discretion of the issuing State or organization, but shall not overlap the portrait area (Zone V) or interfere with the legibility of other data in the VIZ. Font, field and background should conform to the specifications for the MRZ set out in Doc 9303-3.

Further information concerning the technical specifications, derivation and implementation of CANs may be found in Doc 9303-11.

4.2 Machine Readable Zone (MRZ) (Zone VII)

4.2.1 Data position, data elements and print position in the MRZ

4.2.1.1 Data position

The MRZ is located on the front of the MRP data page. Figure 3 defines the location of the MRZ and the nominal position of the data therein.

4.2.1.2 Data elements

The data elements corresponding to Fields 03 to 09, 11 and 16 of the VIZ shall be personalized in machine readable form, in the MRZ, beginning with the left most character position in each field in the sequence indicated in the data structure specifications shown below. Figure 15 indicates the structure of the MRZ.

4.2.1.3 Print position

The position of the left-hand edge of the first character shall be 6.0 ± 1.0 mm (0.24 ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the OCR lines and the minimum starting position for the first character of each line are shown in Figure 3. The positioning of the characters is indicated by those reference lines and by the printing zones for the two code lines in Figure 7.

4.2.2 Data structure of machine readable data for the MRP data page

4.2.2.1 Data structure of the upper machine readable line

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 2	03	Document code	The first character shall be P to designate an MRP. One additional letter may be used, at the discretion of the issuing State or organization, to designate a particular MRP. If the second character position is not used for this purpose, it shall be filled by the filler character (<).	2	Notes a, d, m.
3 to 5	04	Issuing State or organization	The three-letter code specified in Doc 9303-3 shall be used. Spaces shall be replaced by filler characters (<).	3	Notes a, d, f.
6 to 44	06, 07	Name	For details see Doc 9303-3.	39 [Primary identifier(s),	Notes a, c, d.

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
				secondary identifier(s) and fillers]	
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ. For details on apostrophes, hyphens, commas, etc., see Doc 9303-3.		
		Name prefixes and suffixes	For details see Doc 9303-3.		
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 39 characters in total, all name components shall be included in the MRZ and all unused character positions shall be completed with filler characters (<) repeated up to position 44 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 39), they shall be truncated as follows: Characters shall be removed from one or more components of the primary identifier until three character positions are freed, and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 44) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred. Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 44). This indicates that truncation may have occurred.		Notes a, d.

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
			When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 39, characters shall be removed from one or more components of the name until the last character in the name field is an alphabetic character.		

** Notes can be found in the last portion of sub-section 4.2.2.2.*

4.2.2.2 Data structure of the lower machine readable line

MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 9	05	Passport number	As given by the issuing State or organization to uniquely identify the document. Any special characters or spaces in the passport number as shown in the VIZ shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 9 as required.	9	Notes a, b, d.
10		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, d.
11 to 13	08	Nationality	As a three-letter code representing the holder’s nationality as listed in Doc 9303-3. Spaces are replaced by filler characters.	3	Notes a, d, f.
14 to 19	9	Date of birth	See Doc 9303-3 for details.	6	Notes b, d, i.
20		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, d.
21	11	Sex	F = female; M = male; < = unspecified.	1	Notes a, d.

MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
22 to 27	16	Date of expiry	See Doc 9303-3 for details.	6	Notes b, d, i.
28		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, d.
29 to 42	10	Personal number or other optional data elements	Any special characters, including spaces in the personal identification number given to the holder by the issuing State or organization, shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 42 as required. When the personal number field is not used, the character positions 29 to 42 in the second MRZ line should be completed with filler characters (<) (see also under “check digit”, character position 43 below).	14	Notes a, b, d.
43		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4. When the personal number field is not used and filler characters (<) are used in positions 29 to 42, the check digit may be zero or the filler character (<) at the option of the issuing State or organization.	1	Notes b, d.
44		Composite check digit	Composite check digit for characters of machine readable data of the lower line in positions 1 to 10, 14 to 20 and 22 to 43, including values for letters that are a part of the number fields and their check digits. Shall be calculated as specified in Doc 9303-3.	1	Notes b, d.

** Notes to the Visual and Machine Readable data element directories:*

a) Alphabetic characters (A–Z) and (a-z). National characters may be included in the VIZ. In the MRZ only the characters defined in Doc 9303-3 shall be used.

b) Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ only the numerals 0–9 may be used as defined in Doc 9303-3.

.

c) Punctuation may be included in the VIZ. In the MRZ only the filler character specified in Doc 9303-3 may be used.

d) The field caption is not printed on the document.

e) The use of a caption to identify the field is at the option of the issuing State.

f) In the case of the United Nations laissez-passer, Field 01 (Issuing State or Organization) in the VIZ shall be completed with the words “UNITED NATIONS — NATIONS UNIES”. In keeping with the international character of United Nations officials, neither nationality nor place of birth shall be shown. The caption for Field 08 (Nationality) shall read instead: “Official of/Fonctionnaire des” and the words “UNITED NATIONS/ NATIONS UNIES” entered instead of nationality. Field 12 (Place of birth) shall be left blank. The codes to be used in Field 04 (Code for issuing State or organization) in the VIZ as well as in character positions 3 to 5 (Issuing State or Organization) in the upper line of the MRZ and in character positions 11 to 13 (Nationality) in the lower line shall be as specified in Doc 9303-3.

g) A blank space (or spaces) is included. Blank spaces between words shall count towards the maximum number of characters permitted in the field.

h) Intentionally omitted from the Data Element Directory. In the sixth and earlier editions of Doc 9303, this Note provided for stick-in portrait photographs the use of which is no longer permitted in an MRP.

i) The method of writing dates is given in Doc 9303-3.

j) The space reserved for Field 15 may be expanded to include additionally the space for Field 18 when the option is taken of locating the holder’s signature or usual mark on the adjacent page. In this instance, the authority or issuing organization may be expressed as two lines of variable numbers of character positions.

k) When the name cannot be accommodated in the space provided for it in the VIZ, a notation giving the full name may be written on another page of the MRP. Alternatively, a smaller type font may be selected for use in the VIZ only.

l) The field caption shall be printed on the document.

m) In documents other than passports, e.g. United Nations laissez-passer, seafarer’s identity document or refugee travel document, the official title of the document shall be indicated instead of “Passport”. However, the first character of the document code shall be P.

n) In Machine Readable Convention Travel Documents (MRCTDs) the words “Travel Document” shall be indicated instead of “Passport”.

o) In MRCTDs States may include or omit the nationality data element. If nationality is included, it is recommended that States enter “Stateless Person” or “Refugee”. This ensures consistency between the VIZ and the MRZ (where the three-letter code for Stateless Persons – XXA, and for Refugees – XXB, appears).

p) Where an issuing State or organization does not want to identify the sex, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.

4.2.3 Truncation of names in the MRZ

The name field in the MRZ of the MRP allows for a maximum of 39 characters in the upper line. If the primary and secondary identifiers using the above procedure exceed the available character positions, then truncation shall be carried out using the procedure set out in the following paragraphs. If the total number of characters in the name, including filler characters, is 39 or fewer the name shall not be truncated.

In truncating the name components, the last character of the name field shall be an alphabetic character (A to Z inclusive) as an indication that truncation has occurred (see the Data Element Directory of the MRZ in 4.2.2).

Note.— Where long names extend to the last character position in the name field, the presence of an alphabetic character means that the name must be treated as though truncation had occurred.

4.2.3.1 Examples of name of the holder in the MRZ

Note.— In the following examples, the document is assumed to be a passport issued by the State of Utopia. The first five characters of the upper machine readable line are P<UTO.

a) Usual representation:

Name: Anna Maria Eriksson
VIZ: ERIKSSON, ANNA MARIA
MRZ: P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<

b) Central primary identifier:

Name: Deborah Heng Ming Lo
VIZ: HENG, DEBORAH MING LO
MRZ: P<UTOHENG<<DEBORAH<MING<LO<<<<<<<<<<<<<<<<<<

c) Hyphen as part of the name:

Name: Susie Margaret Smith-Jones
VIZ: SMITH-JONES, SUSIE MARGARET
MRZ: P<UTOSMITH<JONES<<SUSIE<MARGARET<<<<<<<<<<<<

d) Apostrophe as part of the name:

Name: Enya Siobhan O’Connor
VIZ: O’CONNOR, ENYA SIOBHAN
MRZ: P<UTOOCONNOR<<ENYA<SIOBHAN<<<<<<<<<<<<<<<<<<

e) Multiple name components:

Name: Martin Van Der Muellen
VIZ: VAN DER MUELLEN, MARTIN
MRZ: P<UTOVAN<DER<MUELLEN<<MARTIN<<<<<<<<<<<<<<<<

Name: Huda Muhammad Jawad Al-Basri
VIZ: AL-BASRI, HUDA MUHAMMAD JAWAD
MRZ: P<UTOAL<BASRI<<HUDA<MUHAMMAD<JAWAD<<<<<<<<<<

Name: Jose Ramon Vilarchao Fernandez
VIZ: VILARCHAO FERNANDEZ, JOSE RAMON
MRZ: P<UTOVILARCHAO<FERNANDEZ<<JOSE<RAMON<<<<<<<<

f) No secondary identifier:

Name: Arkfreith
VIZ: ARKFREITH
MRZ: P<UTOARKFREITH<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Name: Satriya Sudarpa
VIZ: SATRIYA SUDARPA
MRZ: P<UTOSATRIYA<SUDARPA<<<<<<<<<<<<<<<<<<<<<<<

4.2.3.2 Truncated names — Secondary identifier truncated

a) One or more name components truncated to initials:

Name: Nilavadhanananda Chayapa Dejthamrong Krasuang
VIZ: NILAVADHANANANDA, CHAYAPA DEJTHAMRONG KRASUANG
MRZ: P<UTONILAVADHANANANDA<<CHAYAPA<DEJTHAMRONG<K

b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
MRZ: P<UTONILAVADHANANANDA<<ARNPOL<PETCH<CHARONGU

4.2.3.3 Truncated names — Primary identifier truncated

a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ: P<UTOBENNELONG<WOOLOOMOOLOO<WARRANDYTE<W<<DI

b) One or more components truncated:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ: P<UTOBENNELONG<WOOLOOM<WARRAND<WARNAM<<DINGO

c) One or more components truncated to a fixed number of characters:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ: P<UTOBENNEL<WOOLOO<WARRAN<WARNAM<<DINGO<POTO

4.2.3.4 Names that fit into the maximum positions available within in the name field, indicating possible truncation by the letter in the last position, but which are not truncated

Name: Jonathon Warren Trevor Papandropoulous
VIZ: PAPANDROPOULOUS, JONATHON WARREN TREVOR
MRZ: P<UTOPAPANDROPOULOUS<<JONATHON<WARREN<TREVOR

Note.— Even though there is an alphabetic character in the 44th position of this passport upper machine readable line, this name has not been truncated but it must be assumed that it has been truncated.

4.2.4 Check digits in the Machine Readable Zone

The data structure of the lower machine readable line specified in paragraph 4.2.2.2 provides for the inclusion of five check digits as follows:

Check digit	*Character positions (lower MRZ line) used to calculate check digit*	*Check digit position (lower MRZ line)*
Passport number	1-9	10
Date of birth	14-19	20
Date of expiry	22-27	28
Personal number	29-42	43
Composite check digit	1-10, 14-20, 22-43 *Note.— Positions 11-13 and 21 are excluded when calculating the composite check digit.*	44

4.3 Representation of the Issuing State or Organization and Nationality of Holder in the MRZ and the VIZ

Use of three-letter Country codes is mandatory in the MRZ and Field 04 in the VIZ and optional for the holder's nationality in the VIZ. Specific locations are defined in the following table:

	Zone	*Field no.*	*Character position no.*	*Number of character positions*
Issuing State or organization	VIZ	04	3-5	3
	MRZ (upper line)			3
Holder's nationality	VIZ	08	11-13	variable
	MRZ (lower line)			3

5. REFERENCES (NORMATIVE)

ISO/IEC 7810	ISO/IEC 7810:2003, Identification cards – Physical characteristics.
ISO/IEC 18745-1	ISO/IEC 18745-1:2018, Information technology – Test methods for machine readable travel documents (MRTD) and associated devices – Part 1: Physical test methods for passport books (durability).

— — — — — — — —

Appendix A To Part 4

EXAMPLES OF A PERSONALIZED MRP DATA PAGE (INFORMATIVE)

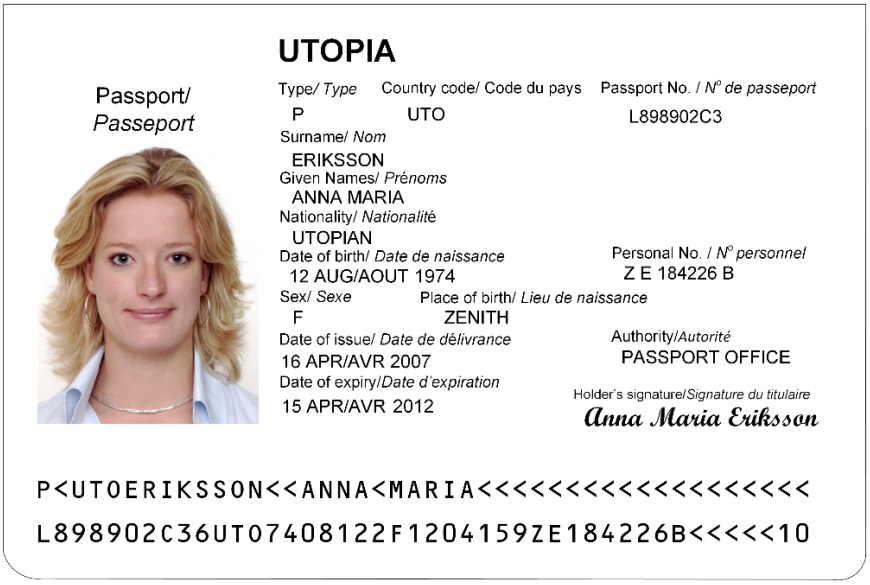


Figure 11. Example of an MRP data page that conforms to the recommended practice layout.

Figure 12. Example of an MRP data page excluding Zone IV (the holder's signature or usual mark) and including a national language and Optional Data Field 13, for optional personal details (e.g. occupation) in Zone II.

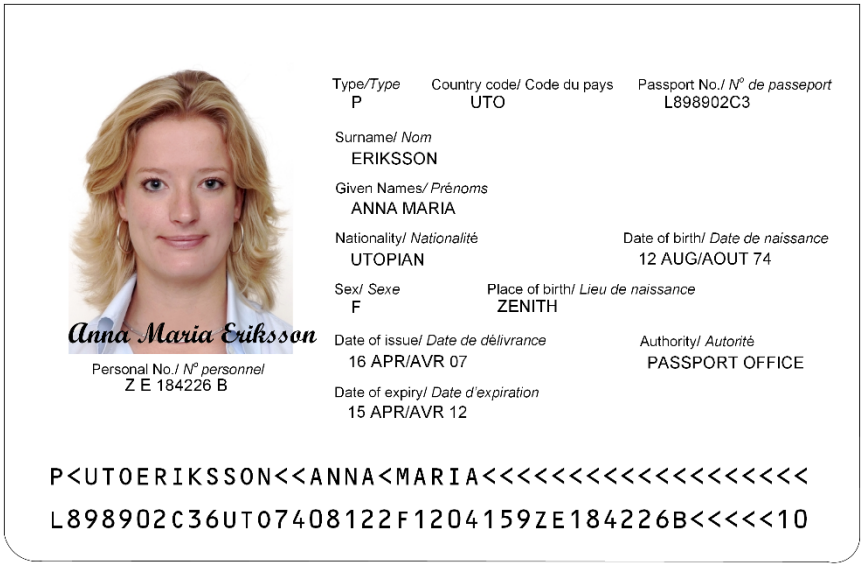


Figure 13. Example of an MRP data page appearing on an interior page of the book. The name of the issuing State or organization and the name of the document have appeared on an earlier page and are therefore omitted from the data page. The example also illustrates Zone V (the portrait) moved vertically upwards with Zone IV (the signature) overlaying the portrait, and the personal number from Zone II placed beneath the portrait.

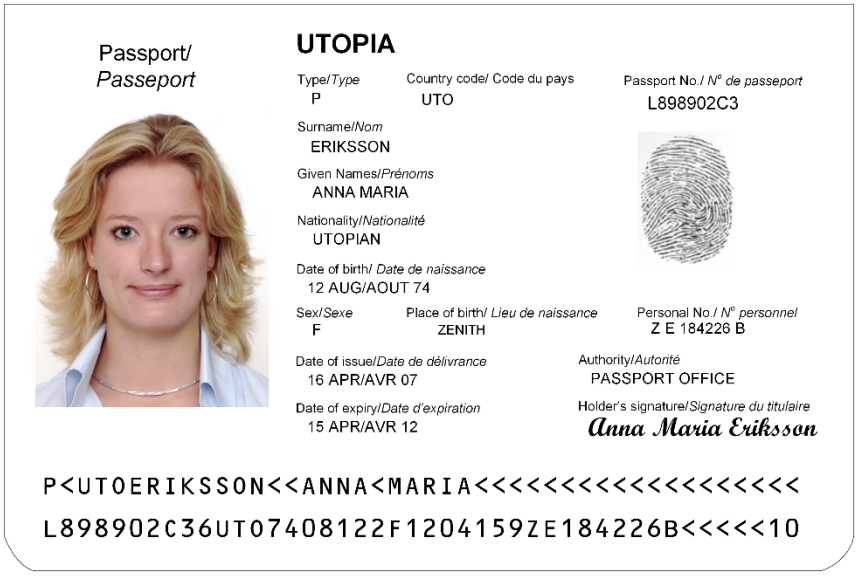


Figure 14. Example of an MRP data page with the layout adjusted to accommodate a displayed fingerprint in Zone II.

— — — — — — — —

Appendix B To Part 4

CONSTRUCTION OF THE MACHINE READABLE ZONE OF THE PASSPORT DATA PAGE (INFORMATIVE)

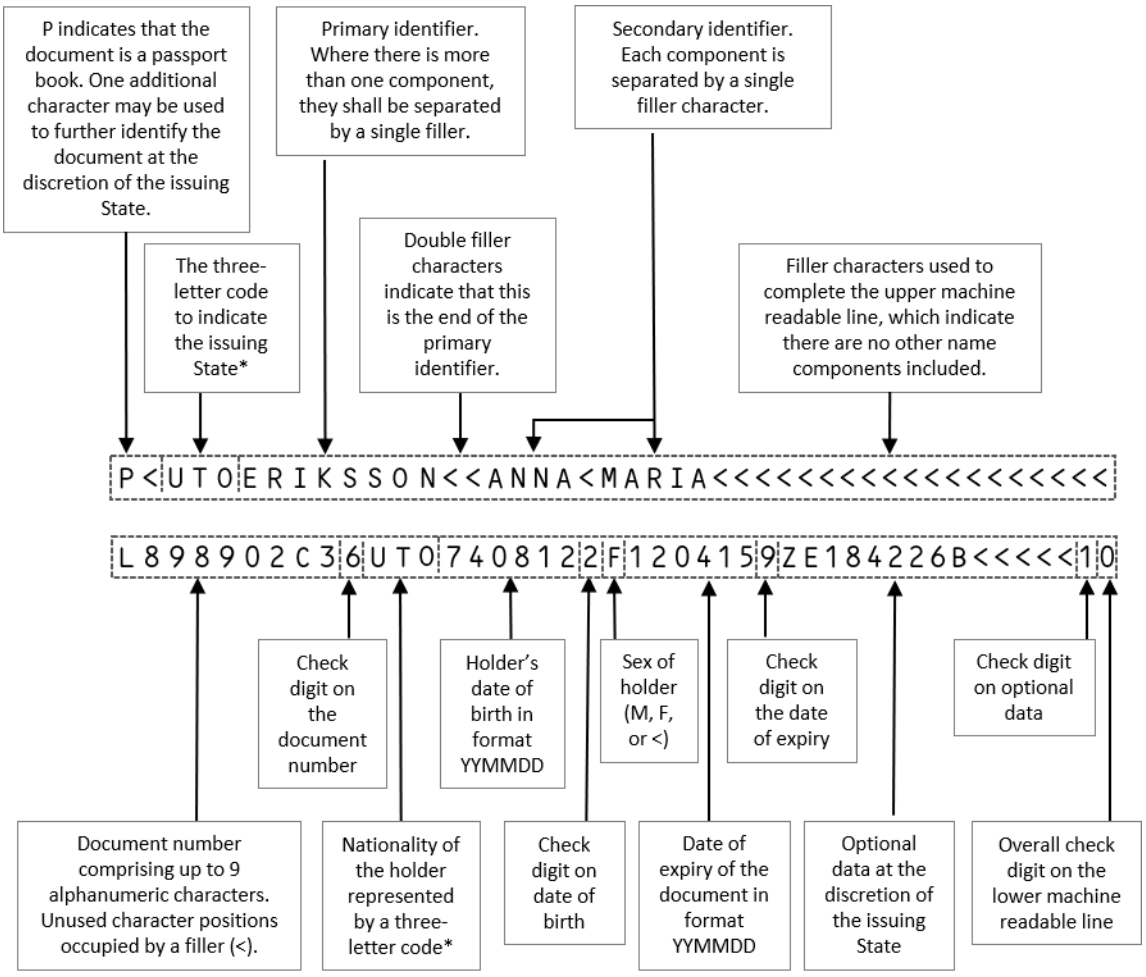


Figure 15. Example showing the sequence and content of data elements in the MRZ

*Note 1.— * Three letter codes are given in Doc 9303-3.*

Note 2.— Dotted lines indicate data fields; these, together with arrows and comment boxes, are shown for the reader's understanding only and are not printed on the document.

Note 3.— Data is inserted into a field beginning at the first character position starting from the left. Any unused character positions shall be occupied by filler characters (<).

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 20XX

Part 5: Specifications for TD1 Size
Machine Readable Official Travel Documents (MROTDs)

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 5 — *Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)*
ISBN 978-92-9249-794-1

DOCUMENT CHANGE RECORD

Doc 9303, Part 5

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

1. SCOPE

Doc 9303-5, defines specifications that are specific to TD1 Size Machine Readable Official Travel documents (MROTDs) and shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*;
- Part 3 — *Specifications Common to all MRTDs*.

Together these specifications provide for global data interchange of MRTDs both by visual (eye readable) and machine readable (optical character recognition) means.

Additional specifications providing for global data interchange of electronic data in eMRPs and eMROTDs may be found in Doc 9303, Parts 9 through 12.

2. DIMENSIONS OF THE TD1 SIZE MROTD

2.1 Nominal Dimensions

The nominal dimensions shall be those specified in ISO/IEC 7810: 2019 for the ID-1 type card:

85.60 mm (3.370 in) wide by 53.98 mm (2.125 in) wide

2.2 Edge Tolerances

The edges of the document after final preparation shall be within the area circumscribed by the concentric rectangles as illustrated in Figure 1.

Inner rectangle: 53.25 mm × 84.85 mm (2.10 in × 3.34 in)
Outer rectangle: 54.75 mm × 86.35 mm (2.16 in × 3.40 in)

In no event shall the dimensions of the finished TD1 document exceed the dimensions of the outer rectangle, including any final preparation (e.g. laminate edges).

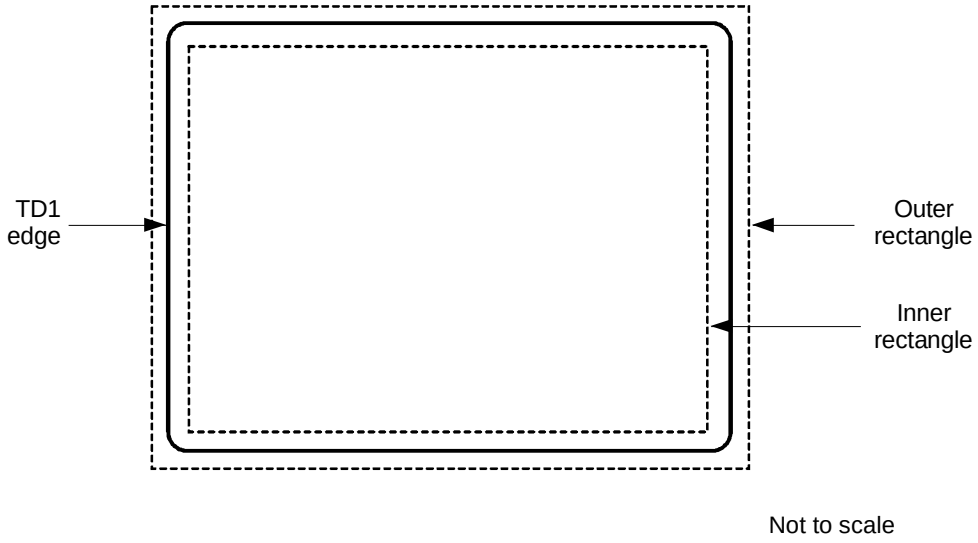


Figure 1. TD1 dimensional illustration

2.3 Margins

The dimensional specifications refer to the outer limits of the TD1. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data. See Figure 2.

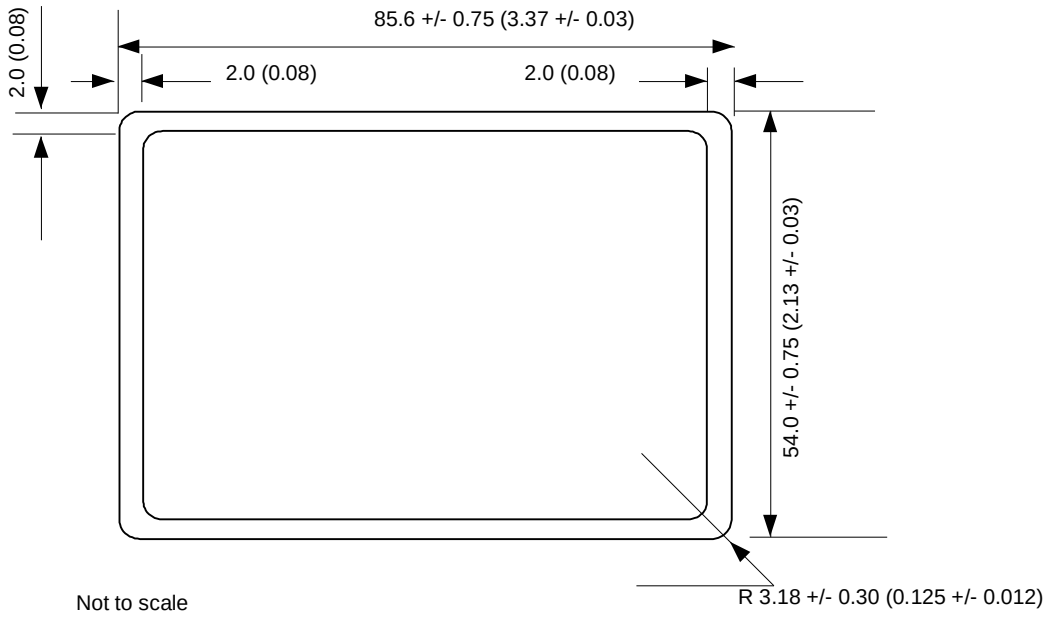


Figure 2. Edge margins and nominal dimensions of a TD1 Size MROTD

2.4 Thickness

The thickness, including any final preparation (e.g. laminate), shall be as follows:

- Minimum:

0.25 mm (0.01 in);

- Maximum:

1.25 mm (0.05 in).

The thickness of the area within the machine readable zone shall not vary by more than 0.1 mm (0.004 in).

Note.— The tolerances specified above differ from those specified in ISO/IEC 7810 for the ID-1 size card. This is for historical reasons; TD1 cards were originally produced using encapsulated pouch card methods which are incapable of achieving the permitted tolerances of ISO/IEC 7810. Some cards may still be produced using these techniques and others where the personalization process renders it impractical to achieve ISO/IEC 7810 tolerances. Wherever possible, however, dimensions and tolerances should conform to ISO/IEC 7810.

General note.— The decimal notation used in these specifications conforms to ICAO practice. This differs from the ISO practice, which is to use a decimal point (.) in imperial measurements and a comma (,) in metric measurements.

3. GENERAL LAYOUT OF THE TD1 SIZE MROTD

The MROTD follows a standardized layout to facilitate reading of data globally by both visual and machine readable means (global interoperability).

3.1 TD1 Zones

To accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements, the MROTD is divided into seven zones as listed below in paragraphs 3.1.1 and 3.1.2. Zones I through VI constitute the visual inspection zone (VIZ). Zone VII is the machine readable zone (MRZ).

The location, contents and dimensional specifications of zones are described below in Sections 3.2 to 3.3.

3.1.1 Front of the TD1

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Mandatory holder's signature or usual mark
Zone V	Mandatory identification feature

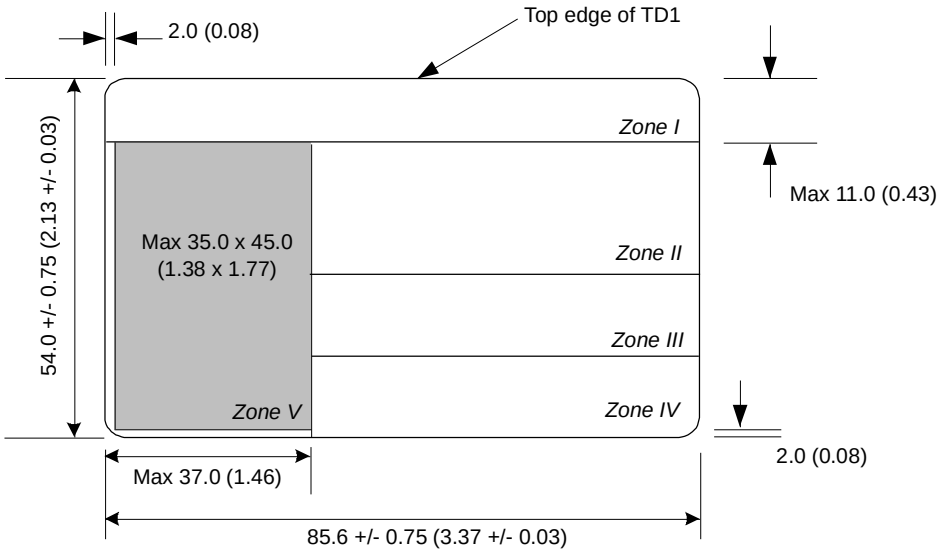


Figure 3. Nominal layout of the zones on the front side of a TD1 Size MROTD

3.1.2 Back of the TD1

Zone VI Optional data elements
Zone VII Mandatory Machine Readable Zone (MRZ)

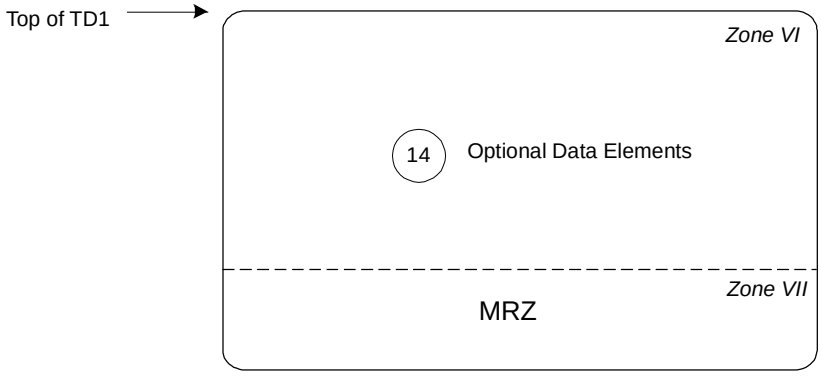


Figure 4. Layout of zones on the reverse side of a TD1

3.2 Content and Use of Zones

The data elements to be included in the zones, the preparation of the zones and guidelines for the dimensional layout of zones shall be as described hereunder.

Zones I to V and Zone VII contain mandatory elements which represent the minimum requirements for the TD1. The optional elements in Zones II, III and VI accommodate the diverse requirements of issuing States or organizations, allowing for presentation of additional data at the discretion of the issuing State or organization, while achieving the desired level of standardization. The location of zones and standard sequence for data elements are shown in Figures 3 to 5. Figures 7 to 9 outline the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States or organizations. Examples of a personalized TD1 are shown in Appendix A, Figures 11 to 14.

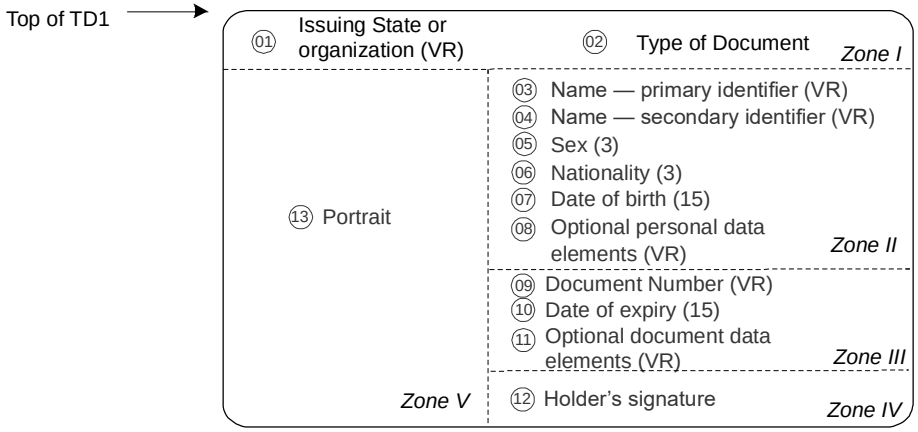


Figure 5. Sequence of data elements on the front side of a TD1

3.2.1 Mandatory zones

Zone I on the front of the MROTD identifies the issuing State or organization and the document.

Data elements shall appear in a standard sequence in Zones II and III. Zones II and III each contain a field in which optional data elements may be included. The optional field in Zone II shall be used for personal data elements and the optional field in Zone III for document-related data elements. Where an issuing State or organization does not use the optional fields in Zones II and III, there is no need to reserve the space for them on the TD1.

Zone IV contains the holder's signature or usual mark. The issuing State or organization shall decide the acceptability of a holder's usual mark.

Zone V shall contain the personal identification feature(s) which shall include a portrait solely of the holder. At the discretion of the issuing State or organization, the name fields in Zone II and the holder's signature or usual mark in Zone IV may overlay Zone V provided this does not hinder recognition of the data in any of the three zones.

The standard position for the holder's portrait is along the left edge of the front of the TD1, as described in Section 3.3 and illustrated in Figure 3.

When an issuing State or organization chooses, for its own or for bilateral purposes, to expand the machine readable data capacity of a TD1 through use of an integrated circuit with contacts, the holder's portrait (Zone V) shall be relocated such that its right edge is coincident with the right edge of the front of the TD1. Zones II, III and IV shall in turn be relocated to have their left edge coincident with the left edge of the front of the TD1. The specifications for Zones II through IV are similar to those defined in Section 3.3, but adjusted to accommodate the relocation of the portrait to the right and to avoid the area containing the contacts of the IC as defined by ISO/IEC 7816-2.

The size of the portrait is given in the Data Element Directory for the Visual Zone, Section 4.1.1.1, Field 13/V.

Zone VII shall contain the machine readable data. Because of the smaller size of the TD1, to accommodate the required data, three lines of machine readable data are included in the MRZ. Detailed specifications for the MRZ of the TD1 are given in Section 4.2. Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the effective reading zone (ERZ) specified in Doc 9303-3.

All MRZ data elements shall be shown in Zone VII. For a TD1 Size MROTD, these are defined in Section 4.2.2 and positioned as shown below.

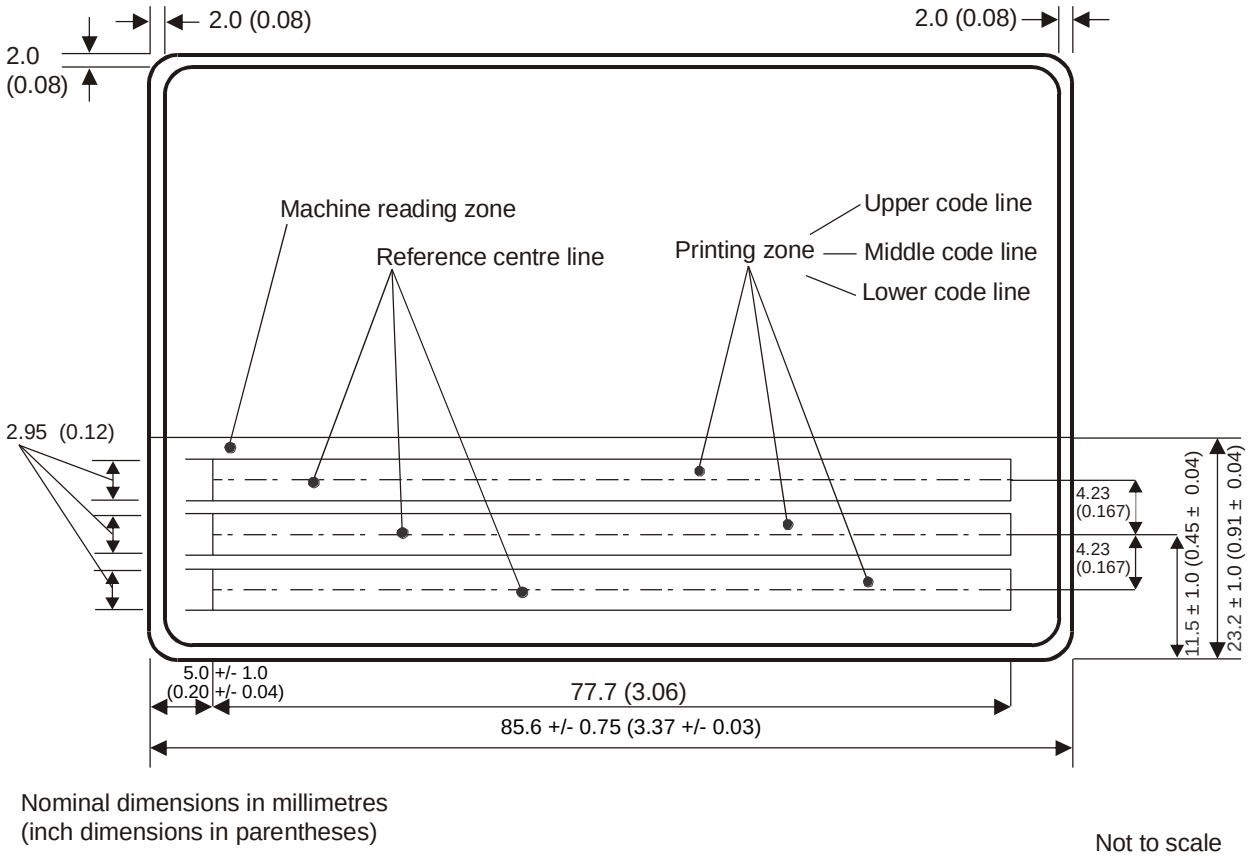


Figure 6. Position and dimensions of Zone VII the Machine Readable Zone

3.2.2 Optional data zone

Zone VI, which appears on the back of the MROTD, is a zone for optional data for use at the discretion of the issuing State or organization. Zone VI will always appear irrespective of whether or not it is used.

3.2.3 Card access number

In the case of TD1 Size MROTDs containing a contactless IC, issuing States or organizations may, at their discretion, wish to include a Card Access Number (CAN) on the front side of the card to facilitate machine reading and data capture

from the card. Specifically, the purpose of the CAN is to enable the front side of the card to be read AND the chip to be accessed without flipping the card to read the MRZ on the rear. When the chip supports PACE V2, this can be accomplished by adding a CAN on the front side of a TD1 Size card. The CAN and its position on the front side of the MROTD are specified as follows.

The CAN is a 6-digit number, comprised solely of numerals, 0 to 9. There is no check digit, since the check is implicitly performed by the protocol. Font, field and background are conforming to the specifications for the MRZ set out in Doc 9303-3. Vertical position is conforming to the vertical position of any one of the three MRZ lines as specified in this document and shown in Figure 6. The horizontal position shall be at the discretion of the issuing State or organization, but shall not overlap the portrait area (Zone V) or interfere with the legibility of other data in the VIZ.

Further information concerning the technical specifications, derivation and implementation of CANs may be found in Doc 9303-11.

3.3 Dimensional Flexibility of Zones I to V

Zones I to V may be adjusted in size and shape within the overall dimensional specifications of the TD1 to accommodate the diverse requirements of issuing States or organizations. All zones, however, shall be bounded by straight lines, and all angles where straight lines join shall be right angles (i.e. 90 degrees). It is recommended that the zone boundaries not be printed on the TD1. Examples of flexible location of the zones are shown in Figures 7 to 10.

When an issuing State or organization chooses to produce a TD1 that contains a transparent or otherwise unprintable border around the card, this will result in a reduction of the available area within the zones. The full TD1 dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the TD1.

Zone I shall be located along the top edge of the TD1 and extend across the full width of the document. The issuing State or organization may vary the *vertical* dimension of Zone I, as required, but this dimension shall be sufficient to allow legible interpretation of the data elements in the zone and shall not be greater than 11.0 mm (0.43 in).

Zone V shall be located such that its left edge is coincident with the left edge of the TD1. Zone V may vary in size but shall not exceed the maximum dimensions specified in Figure 10.

Zone V may move *vertically* along the left edge of the TD1 and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. The scope for such movement is illustrated in Figure 10. When the printed photograph occupies the maximum area of 35mm x 45mm within Zone V, an additional horizontal tolerance up to 2mm is allowable.

The upper boundary of Zone II shall be coincident with the lower boundary of Zone I.

When there is a specific requirement for the name field to extend across the TD1, Zone II may extend up to the full width of the TD1 as illustrated in Figure 13. In the event the full dimension is used, Zone II shall overlay a portion of Zone V. In this case, issuing States or organizations shall ensure that data contained in either zone are not obscured. Figures 8 and 10 illustrate a Zone II design less than the full dimensional width of the document.

The lower boundary of Zone II may be positioned at the discretion of the issuing State or organization. Enough space must be left for Zones III and IV below the boundary. This boundary does not need to be straight across the longer dimension of the TD1. Figure 9 illustrates a Zone II with the lower boundary on two levels. The flexible design for the Zone II illustrated conforms with the specifications defined above.

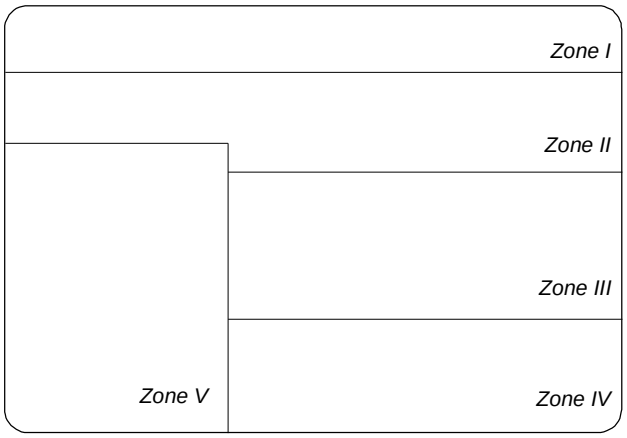


Figure 7. Flexible zone layout with Zone II extending above the portrait

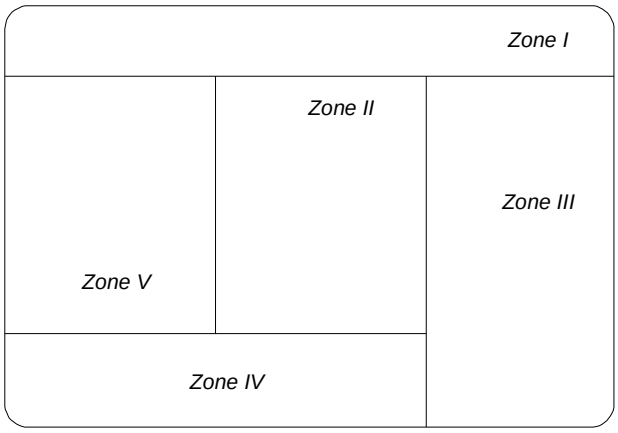


Figure 8. Flexible zone layout with Zone IV, Signature, beneath the portrait

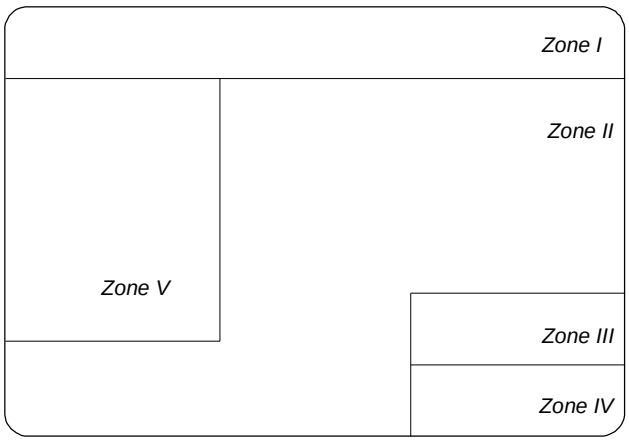


Figure 9. Flexible zone layout with Zone II extending beneath the portrait

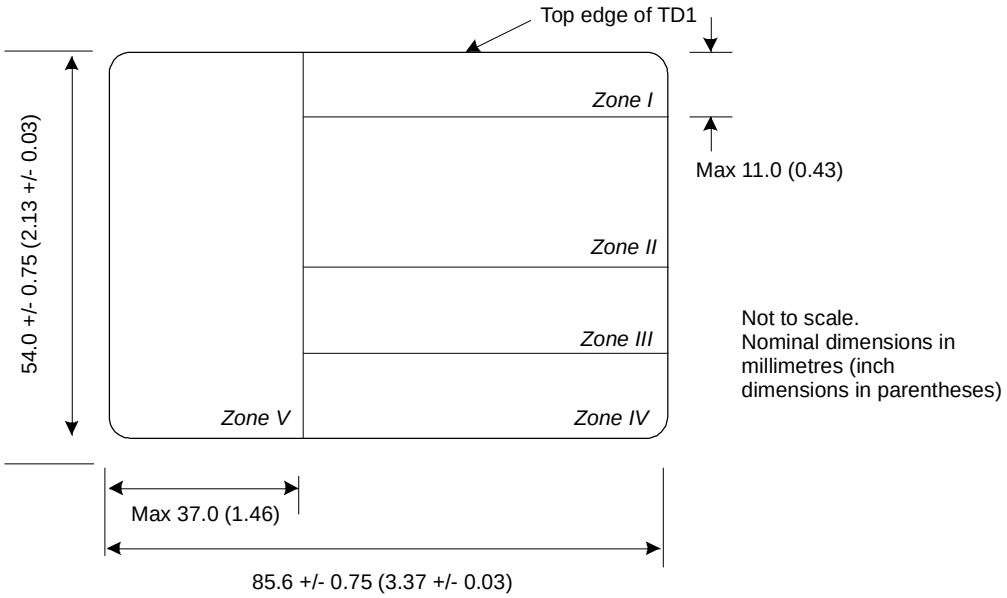


Figure 10. Alternate layout showing flexibility for Zone V to overlay a portion of Zone I

Zone III may start at the right vertical boundary of Zone V and may extend, at the discretion of the issuing State or organization, to the right edge of the TD1. Figures 7 to 9 illustrate some options for a flexible layout of Zone III.

The position of Zone IV is illustrated in the above diagrams, Figures 7 to 10 and in the examples in Appendix A, Figures 11 and 13. Zone IV may overlay Zone V, as illustrated in Figure 13, although this is not recommended practice. In this case, issuing States or organizations shall ensure that individual details contained in either zone are not obscured.

4. CONTENTS OF A TD1 SIZE MROTD

4.1 Visual Inspection Zone (VIZ) (Zones I through VI)

All data in the VIZ shall be clearly legible.

Guidance on the typeface, size and line spacing, the languages and character set to be used in the VIZ may be found in Doc 9303-3.

If any optional field or data element is not used, the data may be spread more evenly in the visual zone of the TD1 consistent with the requirement for sequencing zones and data elements.

4.1.1 Data element directory

4.1.1.1 Visual inspection zone — Data element directory

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
01/I (Mandatory)	Issuing State or organization	The name of the State or organization responsible for issuing the travel document shall be displayed. See Doc 9303-3 for further details.	Variable	Notes a, c, e, h, i.
02/I (Mandatory)	Document	The type or designation of the document. For additional details see Doc 9303-3.	Variable	Notes a, b, c, e, i.
03/04/II (Mandatory)	Name	The full name of the holder, as identified by the issuing State or organization. For additional details see Doc 9303-3.	Variable	Notes a, c, i, l.
03/II (Mandatory)	Primary Identifier	Predominant component(s) of the name of the holder as described in Doc 9303-3. In cases where the predominant component(s) of the name of the holder (e.g. where this consists of composite names) cannot be shown in full or in the same order, owing to space limitations of Field(s) 03 and/or 04 or national practice, the most important component(s) (as determined by the State or organization) of the primary identifier shall be inserted.	Variable	Notes a, c, i, l.
04/II (Mandatory)	Secondary identifier	Secondary component(s) of the name of the holder, as described in Doc 9303-3. The most important component(s) (as determined by the State or organization) of the secondary identifier of the holder shall be inserted in full, up to the maximum dimensions of the field frame. Other components, where necessary, may be represented by initials. Where the holder's name has only predominant component(s), this data field shall be left blank. The State or organization may optionally utilize the whole zone comprising Fields 03 and 04 as a single field. In such a case the primary identifier shall be placed first, followed by a comma and a space, followed by the secondary identifier.	Variable	Notes a, c, i, l.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
05/II (Mandatory)	Sex	Sex of the holder, to be specified by use of the single initial commonly used in the language of the State or organization where the document is issued and, if translation into English, French or Spanish is necessary, followed by an oblique and the capital letter F for female, M for male, or X for unspecified.	3	Notes a, c, f, i, l.
06/II (Mandatory)	Nationality	For details see Doc 9303-3.	Variable	Notes a, h, l.
07/II (Mandatory)	Date of birth	Holder's date of birth as recorded by the issuing State or organization. For unknown dates see Doc 9303-3.	15	Notes a, b, c, i, l.
08/II Optional element in mandatory zone	Optional personal data elements	Optional personal data elements, e.g. personal identification number or fingerprint, at the discretion of the issuing State or organization. If a fingerprint is included in this field, it should be presented as a 1:1 representation of the original. If a date is included, it shall follow the form of presentation described in Doc 9303-3.	Variable	Notes a, b, c, d, g, i.
09/III (Mandatory)	Document Number	As given by the issuing State or organization, to uniquely identify the document from all other MRTDs issued by the State or organization. For additional details see Doc 9303-3.	Variable	Notes a, b, c, i, j, l.
10/III (Mandatory)	Date of expiry	Date of expiry of the document. For additional details see Doc 9303-3.	15	Notes a, b, c, i, l.
11/III Optional element in mandatory zone	Optional document data elements	Optional data elements relating to the document. For additional details see Doc 9303-3.	Variable	Notes a, b, c, d, g, i.
12/IV (Mandatory)	Holder's signature or usual mark	Signature or usual mark of the holder. For additional details see Doc 9303-3.		Note e.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
13/V (Mandatory)	Identification feature	This field shall contain a portrait of the holder. The portrait shall not be larger than 45.0 mm × 35.0 mm (1.77 in × 1.38 in) nor smaller than 32.0 mm × 26.0 mm (1.26 in × 1.02 in). The position of the field concerned shall be along the left edge of the front of the TD1 except where a State or organization chooses to incorporate an integrated circuit with contacts (See Section 3.2.1). See Doc 9303-3 for additional specifications for the portrait.		Note e.
14/VI (Optional)	Optional data elements	Additional optional data elements at the discretion of the issuing State or organization. For additional details see Doc 9303-3.		Notes a, b, c, d, g, i.

** Notes can be found in the last portion of sub-section 4.2.2.3.*

4.2 Machine Readable Zone (MRZ) (Zone VII)

4.2.1 Data position, data elements and print position in the MRZ

4.2.1.1 Data position

The MRZ is located on the back of the TD1. Figure 6 shows the nominal dimensions and position of the data in the MRZ.

4.2.1.2 Data elements

The data elements corresponding to specified fields of the VIZ shall be printed, in machine readable form, in the MRZ, beginning with the left most character position in each field in the sequence indicated in the data structure specifications. Appendix B, Figure 15 indicates the structure of the MRZ.

4.2.1.3 Print position

The position of the left-hand edge of the first character shall be 5.0 ± 1.0 mm (0.20 ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the OCR lines and a nominal starting position for the first character of each line are shown in Figure 6. The positioning of the characters is indicated by those reference lines and by the printing zones of the three code lines in Figure 6.

4.2.2 Data structure of machine readable data for the TD1

4.2.2.1 Data structure of the upper machine readable line

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 2	02	Document code	Two characters, the first of which shall be A, C or I, shall be used to designate the particular type of document. The second character shall be as specified in Note k.	2	Notes a, b, c, e, k.
3 to 5	01	Issuing State or organization	The three-letter code specified in Doc 9303-3 shall be used. Spaces shall be replaced by filler characters (<).	3	Notes a, c, e.
6 to 14	09	Document number	As given by the issuing State or organization, to uniquely identify the document from all other MROTDs issued by the State or organization. Spaces shall be replaced by filler characters (<). For additional details see Doc 9303-3.	9	Notes a, b, e, j.
15		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, c, j.
16 to 30	8, 11 or Zone VI	Optional data elements	For optional use. Unused character positions shall be completed with filler characters (<) repeated up to position 30 as required.	15	Notes a, b, c, e, j.

** Notes can be found in the last portion of sub-section 4.2.2.3.*

4.2.2.2 Data structure of the middle machine readable line

MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 6	07	Date of birth	For details see Doc 9303-3.	6	Notes b, c, e.
7		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b.
8	05	Sex	F = female; M = male; < = unspecified.	1	Notes a, c, e, f.
9 to 14	10	Date of expiry	For details see Doc 9303-3.	6	Notes b, e.
15		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b.
16 to 18	06	Nationality	For details see Doc 9303-3.	3	Notes a, c, e, h.
19 to 29	08, 11 or Zone VI	Optional data elements	For use of the issuing State or organization. Unused character positions shall be completed with filler characters (<) repeated up to position 29 as required. For additional details see Doc 9303-3.	11	Notes a, b, c, e.
30		Composite check digit	Composite check digit to verify the data element of the upper and middle machine readable lines. Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b.

Notes can be found in the last portion of sub-section 4.2.2.3.

4.2.2.3 Data structure of the lower machine readable line

MRZ character positions (line 3)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 30	03, 04	Name	The name consists of primary and secondary identifiers which shall be separated by two filler characters (<<). Components within the primary or secondary identifiers shall be separated by a single filler character (<).	30 (Primary identifier(s), secondary identifier(s) and fillers)	Notes a, c, e.
			When the name of the document holder has only one part, it shall be placed first in the character positions for the primary identifier, filler characters (<) being used to complete the remaining character positions of the MRZ. For additional details see Doc 9303-3.		
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ. For details on apostrophes, hyphens, commas, etc., see Doc 9303-3.		
		Name prefixes and suffixes	For details see Doc 9303-3.		
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 30 characters in total, all permitted name components shall be included in the MRZ, and all unused character positions shall be completed with filler characters (<) repeated up to position 30 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 30), they shall be truncated as follows:		Notes a, c, e and 4.2.3.

MRZ character positions (line 3)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
			Characters shall be removed from one or more components of the primary identifier until three character positions are freed and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 30) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred. Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 30). This indicates that truncation may have occurred. αWhen the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 30, characters shall be removed from one or more components of the name until the last character in the name field is an alphabetic character.		

*Notes relating to paragraphs 4.1.1 and 4.2.2.

a) Alphabetic characters (A–Z) and (a-z). National characters may be included in the VIZ. In the MRZ only the characters defined in Doc 9303-3 shall be used.

b) Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ only the numerals 0–9 may be used as defined in Doc 9303-3.

c) Punctuation may be included in the VIZ. In the MRZ only the filler character specified in Doc 9303-3 may be used.

d) Optional data elements may appear in Zone VI.

e) The field caption is not printed on the document.

f) Where an issuing State or organization does not want to identify the sex, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.

g) The use of a caption to identify a field is at the option of the issuing State or organization.

h) In the case of a document issued by the United Nations Organization, or one of its specialized agencies, to a designated official, the appropriate organization code is used in lieu of nationality. See Doc 9303-3.

i) Blank spaces between words shall count towards the maximum number of characters permitted in the field.

j) The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 6 to 14. They shall be followed by a filler character instead of a check digit to indicate a truncated number. The remaining characters of the document number shall be shown at the beginning of the field reserved for optional data elements (character positions 16 to 30 of the upper machine readable line) followed by a check digit and a filler character.

k) The first character shall be A, C or I. Historically these three characters were chosen for their ease of recognition in the OCR-B character set. The second character shall be at the discretion of the issuing State or organization except that i) V shall not be used, ii) I shall not be used after A (i.e. AI), iii) C shall not be used after A (i.e. AC) except in the crew member certificate.

l) The field caption shall be printed on the document.

4.2.3 Truncation of names in the MRZ

The basic rules for writing the name of the holder in the VIZ and the MRZ appear in ICAO Doc 9303-3. Where the name contains more characters than are available in the name field of the MRZ of the TD1, it is necessary to truncate the name. The following methods provide a number of options available for use at the discretion of the issuing State or organization.

4.2.3.1 Truncated names — Secondary identifier truncated

a) One or more name components truncated to initials:

Name: Nilavadhanananda Chayapa Dejthamrong Krasuang
VIZ: NILAVADHANANANDA, CHAYAPA DEJTHAMRONG KRASUANG
MRZ (lower line): NILAVADHANANANDA<<CHAYAPA<DE<K

b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
MRZ (lower line): NILAVADHANANANDA<<ARNPOL<PE<CH

4.2.3.2 Truncated names — Primary identifier truncated

a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (lower line): BENNELONG<WOOLOOMOOLOO<W<W<<DI

b) One or more components truncated:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (lower line): BENNELONG<WOOLOOM<WA<WARN<<D<P

c) One or more components truncated to a fixed number of characters:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (lower line): BENNE<WOOLO<WARRA<WARNA<<DIN<P

4.2.3.3 Names that fit into the maximum positions available within in the name field, indicating possible truncation by the letter in the last position, but which are not truncated

Name: Jonathon Alec Papandropoulous
VIZ: PAPANDROPOULOUS, JONATHON ALEC
MRZ (lower line): PAPANDROPOULOUS<<JONATHON<ALEC

Note.— Even though there is an alphabetic character in the 30th character position of this TD1 lower machine readable line, this name has not been truncated, but it must be assumed that it has been truncated.

4.2.3.4 Names that contain multiple components

Name: Martin Van Der Muellen
VIZ: VAN DER MUELLEN, MARTIN
MRZ (lower line): VAN<DER<MUELLEN<<MARTIN<<<<<<<

Name: Huda Muhammad Jawad Al-Basri
VIZ: AL-BASRI, HUDA MUHAMMAD JAWAD
MRZ (lower line): AL<BASRI<<HUDA<MUHAMMAD<JAWAD<

Name: Jose Ramon Vilarchao Fernandez
VIZ: VILARCHAO FERNANDEZ, JOSE RAMON
MRZ (lower): VILARCHAO<FERNANDEZ<<JOSE<RAMO

4.2.3.5 No secondary identifier

Name: Arkfreith
VIZ: ARKFREITH
MRZ (lower line): ARKFREITH<<<<<<<<<<<<<<<<<<<<

Name: Satriya Sudarpa
VIZ: SATRIYA SUDARPA
MRZ (lower line): SATRIYA<SUDARPA<<<<<<<<<<<<<<

4.2.4 Check digits in the MRZ

The method of calculating check digits is given in Doc 9303-3. For the TD1, the data structure of the machine readable lines in Paragraph 4.2.2 provides for the inclusion of four check digits as follows:

Check digit	*Character positions (upper MRZ line) used to calculate check digit*	*Check digit position (upper MRZ line)*
Document number check digit	6 – 14	15
or		
Long document number check digit	6-14, 16-28 *Note: position 15 contains '<' and is excluded from the check digit calculation. The position of the last digit of a long document number is in the range of 16-28.*	17,18….or 29 *Note: Since the check digit follows the last digit of the document number its position is in the range of 17-29. The check digit is followed by '<'.*

Check digit	*Character positions (middle MRZ line) used to calculate check digit*	*Check digit position (middle MRZ line)*
Date of birth check digit	1 – 6	7
Date of expiry check digit	9 – 14	15

Check digit	*Character positions (upper/middle MRZ line) used to calculate check digit*	*Check digit position* (*middle MRZ line*)
Composite check digit	6 – 30 (upper line), 1 – 7, 9 – 15, 19 – 29 (middle line) *Note.— Positions 1 – 5 (upper line), positions 8, 16 – 18 (middle line) and positions 1 – 30 (lower line) are excluded in calculating the composite check digit.*	30

4.3 Representation of the Issuing State or Organization and Nationality of the Holder in the MRZ and the VIZ

Use of the three-letter codes listed in Doc 9303-3 is mandatory in the MRZ. In the VIZ, the name of the issuing State or organization shall appear in full; the holder's nationality in the VIZ may appear either in full or in the form of the three-letter code. Specific locations are defined in the following table:

	Zone	*Field no.*	*Character position no.*	*Number of character positions*
Issuing State or organization	VIZ MRZ (upper line)	01	– 3 – 5	Variable 3
Holder's nationality	VIZ MRZ (middle line)	06	– 16 – 18	Variable 3

5. REFERENCES (NORMATIVE)

ISO/IEC 7810	ISO/IEC 7810:2003, Identification cards – Physical characteristics
ISO/IEC7816-2	ISO/IEC7816-2:2007 Cards with contacts — Dimensions and location of the contacts
ISO 1073-2	ISO 1073-2:1976 -- Alphanumeric Character Sets for Optical Recognition CS Part 2: Character set OCR-B -- Shapes and dimensions of the printed image
IATA Airline Coding Directory (ACD)	Published as an e-document by the International Air Transport Association
ICAO Doc 8585	Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services

— — — — — — — —

Appendix A to Part 5

EXAMPLES OF A PERSONALIZED TD1 SIZE MROTD (INFORMATIVE)

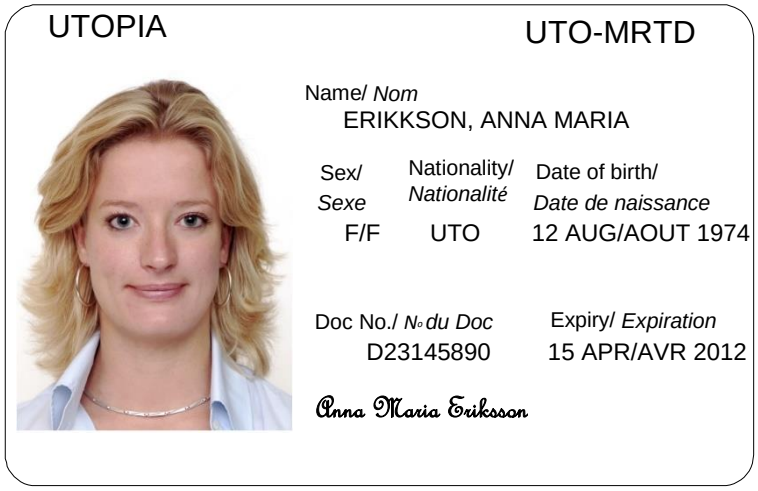
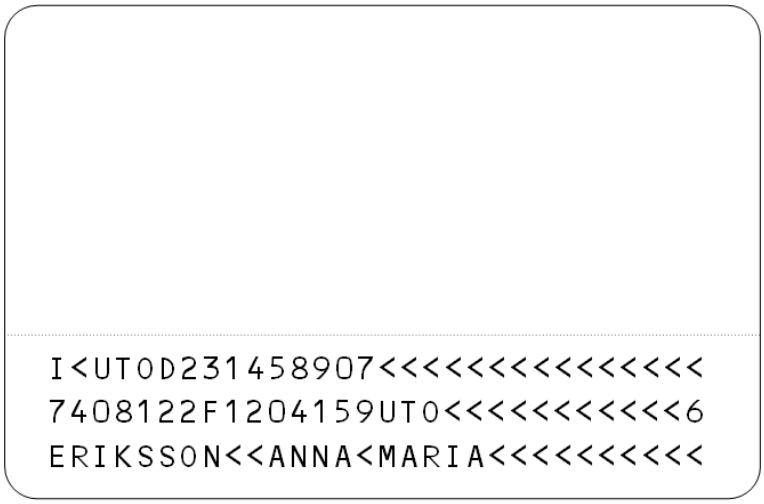


Figure 11. Front side of a TD1 size MROTD with nominal layout with no zone overlaying another



Not to scale

Figure 12. Reverse sde of a TD1 size MROTD showing the MRZ and with no optional document data elements

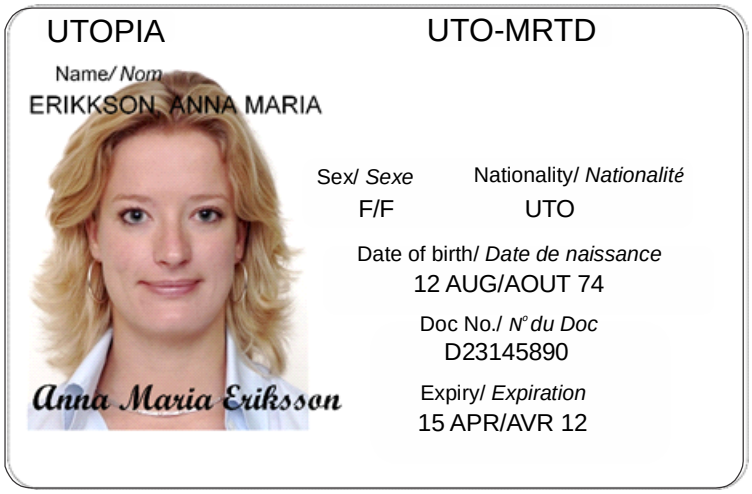
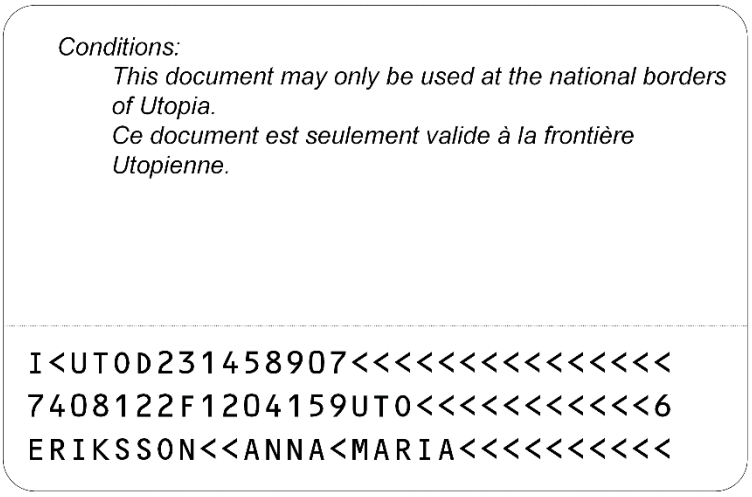


Figure 13. Front side of a TD1 Size MROTD with Zones II and IV overlaying the portrait, Zone V



Not to scale

Figure 14. Reverse side of a TD1 Size MROTD showing the MRZ and including a condition in Zone VI, the Optional Document Data Element zone

— — — — — — — —

Appendix B to Part 5

CONSTRUCTION OF THE MACHINE READABLE ZONE OF A TD1 SIZE MROTD (INFORMATIVE)

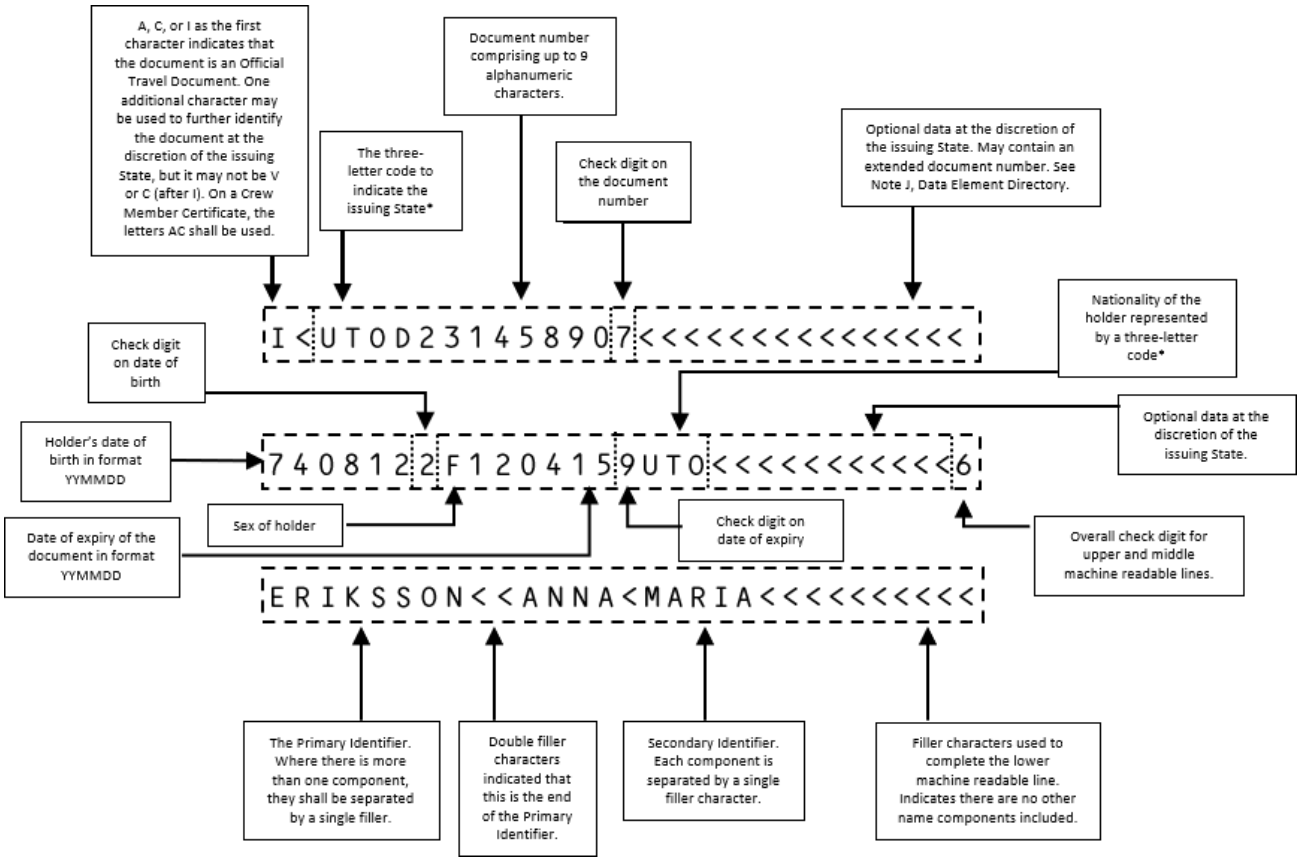


Figure 15. Construction of the 3-line MRZ data on a TD1 Size MROTD

Note 1.— (*) Three-letter codes are given in Doc 9303-3.
Note 2.— Dotted lines indicate data fields; these, together with arrows and comments boxes, are shown for the reader's understanding only and are not printed on the document.
Note 3.— Data is inserted into a field beginning at the first character position starting from the left. Any unused character positions shall be occupied by filler characters (<).

— — — — — — —

Appendix C to Part 5

TECHNICAL SPECIFICATIONS FOR A MACHINE READABLE CREW MEMBER CERTIFICATE – CMC (INFORMATIVE)

C.1 SCOPE

This Appendix defines the modifications to the TD1 specifications necessary to produce a Crew Member Certificate (CMC).

C.2 CONTENT AND USE OF ZONES

The layout of the seven zones and the data elements to be included in the zones shall be as specified in the Data Element Directories for a TD1 Size MROTD as described in this document, with the following modifications:

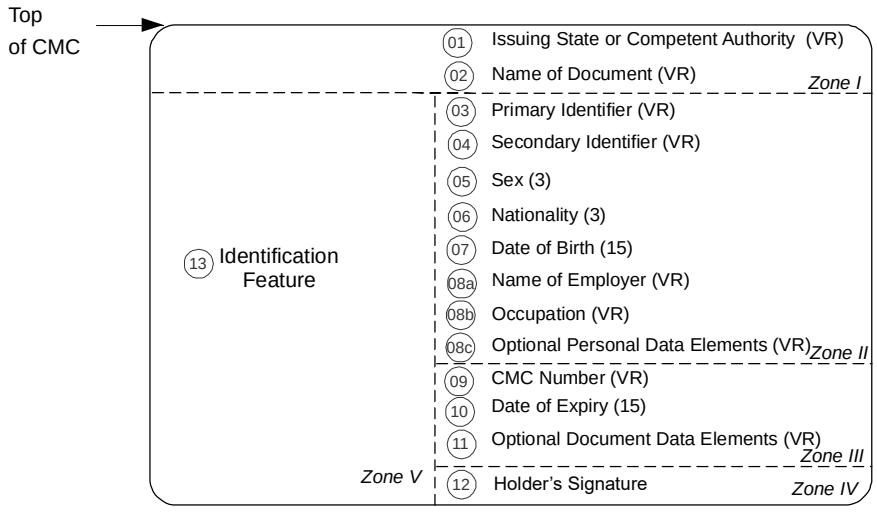
In Zone I, Field 1, the identification of the issuing authority or office may be entered below the name of the State.

In Zone I, Field 2, the type of document, i.e. crew member certificate, shall be entered in the national language of the State in which the document is issued, together with its translation into English, French or Spanish.

In Zone II, in addition to the personal data specified in the TD1, the name of the CMC holder's employer and the holder's employment classification, e.g. pilot or flight attendant, shall be entered.

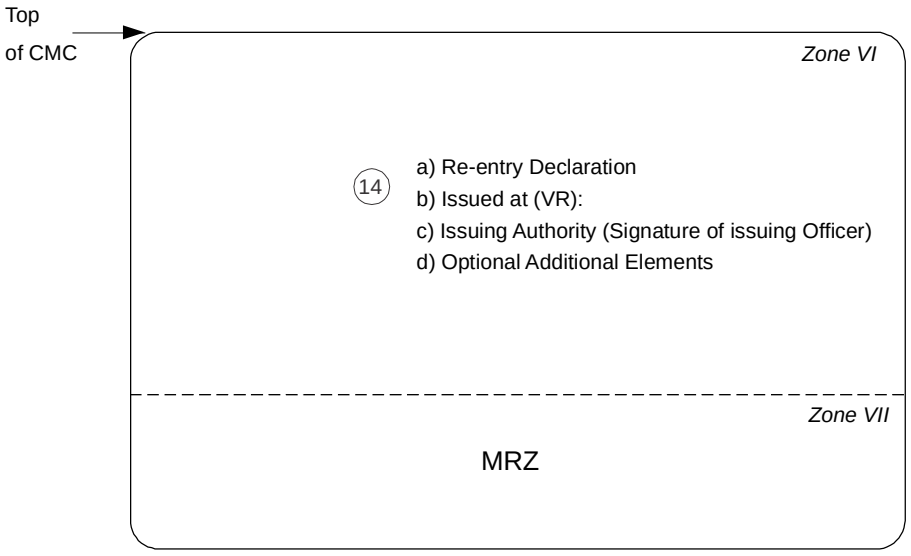
In Zone VI, additional details of the holder's travel status may be entered.

In Zone VII (MRZ), the first two (2) characters in the upper machine readable line, defining the type of document, shall be AC. Characters in positions 16, 17 and 18 in the upper line shall identify the holder's employer using the two-character code specified in the IATA *Airline Coding Directory*, followed by a filler character. Alternatively, characters in positions 16, 17 and 18 shall be the three-letter code specified in ICAO Doc 8585, *Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services.*



Not to scale

Figure 16. Layout of zones and data elements on the front side of a Crew Member Certificate



Not to scale

Figure 17. Layout of zones and data elements on the reverse side of a Crew Members Certificate

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 20XX

Part 6: Specifications for TD2 Size
Machine Readable Official Travel Documents (MROTDs)

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 6 — *Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)*
ISBN 978-92-9249-795-8

DOCUMENT CHANGE RECORD

Doc 9303, Part 6

DATE	NO.	SECTION/PAGES AFFECTED

Page

TABLE OF CONTENTS

1. SCOPE

Note - Recognizing that States or organizations have standardized on the TD1 sized MROTD in lieu of the TD2 format, ICAO will no longer maintain the TD2 specifications beyond the 8th edition of Doc 9303.

Doc 9303-6 defines specifications that are specific to TD2 Size Machine Readable Official Travel Documents (MROTDs) and shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*;
- Part 3 — *Specifications common to all MRTDs*.

Together these specifications provide for global data interchange of MRTDs both by visual (eye readable) and machine readable (optical character recognition) means.

Additional specifications providing for global data interchange of electronic data in eMRPs and eMROTDs may be found in Doc 9303, Parts 9 through 12.

2. DIMENSIONS OF THE TD2 SIZE MROTD

2.1 Dimensions

The dimensions shall be guided by those in ISO/IEC 7810: 2019 (except thickness) for the ID-2 type card:

105.00 mm (4.134 in) wide by 74.00 mm (2.913 in) high

2.2 Edge Tolerances

Inner rectangle: 73.25 mm × 104.25 mm (2.88 in × 4.10 in)
Outer rectangle: 74.75 mm × 105.75 mm (2.94 in × 4.16 in)

In no event shall the dimensions of the finished TD2 document exceed the dimensions of the outer rectangle, including any final preparation (e.g. laminate edges). See Figure 1.

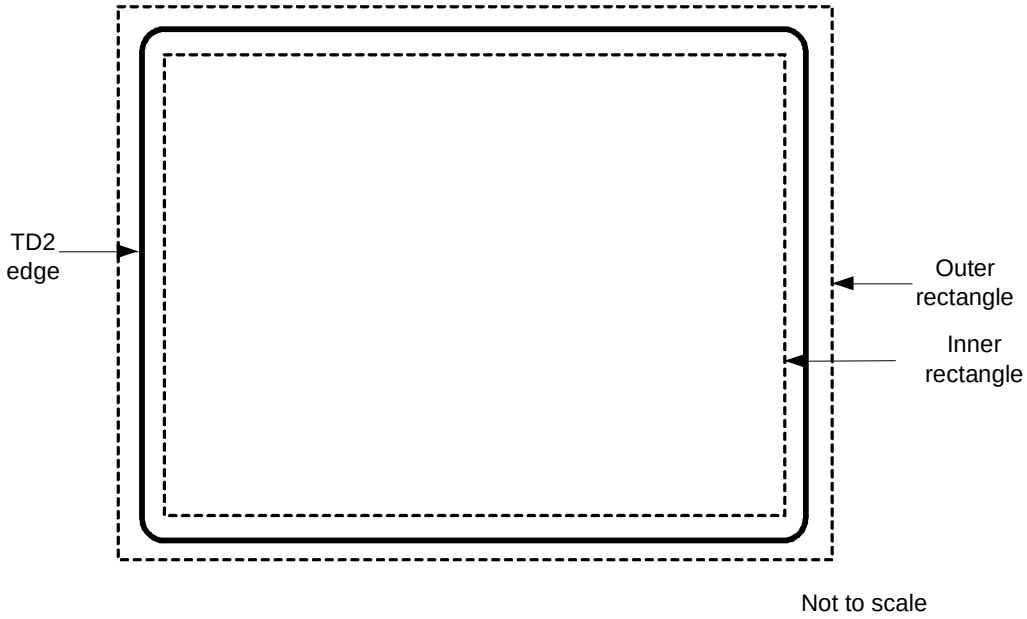


Figure 1. TD2 dimensional illustration

2.3 Margins

The dimensional specifications refer to the outer limits of the TD2. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data. See Figure 2.

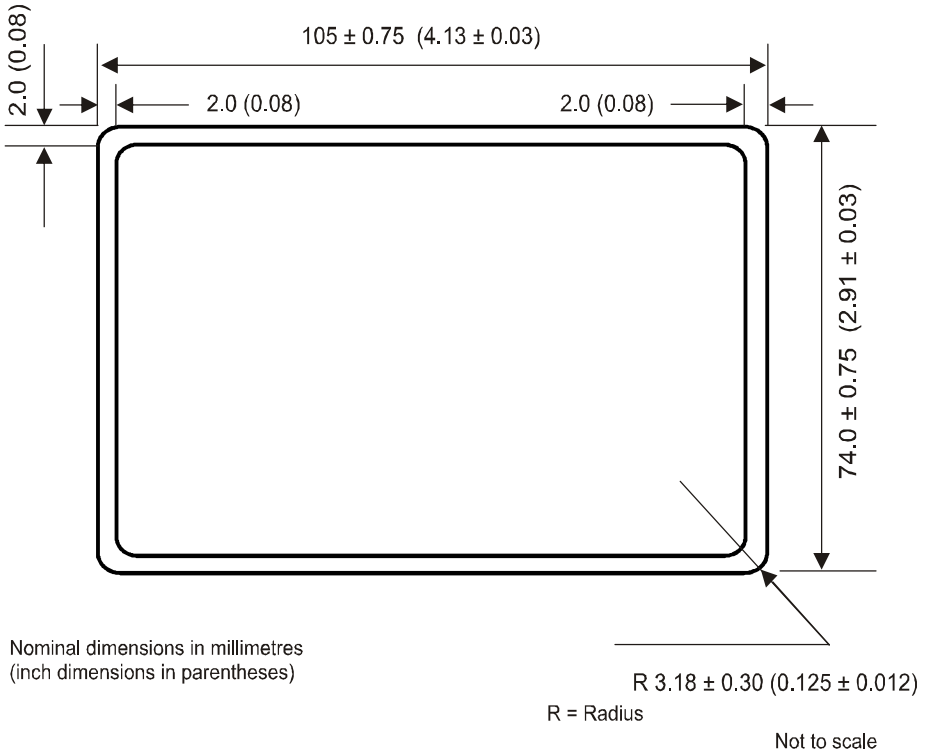


Figure 2. Edge margins and nominal dimensions of a TD2 Size MROTD

2.4 Thickness

The thickness, including any final preparation (e.g. laminate), shall be as follows:

• Minimum:

0.25 mm (0.01 in);

• Maximum:

1.25 mm (0.05 in).

The thickness of the area within the machine readable zone shall not vary by more than 0.1 mm (0.004 in).

Note.— The dimensions and the tolerances specified above differ slightly from those specified in ISO/IEC 7810. This is for historical reasons; TD2 cards were originally produced using encapsulated pouch card methods which are incapable of achieving the permitted tolerances of ISO/IEC 7810. Some cards may still be produced using these techniques and others where the personalization process is incapable of achieving the tight tolerances ISO/IEC 7810 requires. Wherever possible, however, dimensions and tolerances should conform to ISO/IEC 7810.

General note.— The decimal notation used in these specifications conforms to ICAO practice. The ISO practice is to use a decimal point (.) in imperial measurements and a comma (,) in metric measurements.

3. GENERAL LAYOUT OF THE TD2 SIZE MROTD

The TD2 follows a standardized layout to facilitate reading of data globally by both visual and machine readable means (global interoperability).

3.1 TD2 Zones

To accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements, the TD2 is divided into seven zones as listed below in paragraphs 3.1.1 and 3.1.2. Zones I through VI constitute the visual inspection zone (VIZ). Zone VII is the machine readable zone (MRZ).

3.1.1 Front of the TD2

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Mandatory holder's signature or usual mark
Zone V	Mandatory identification feature
Zone VII	Mandatory machine readable zone (MRZ)

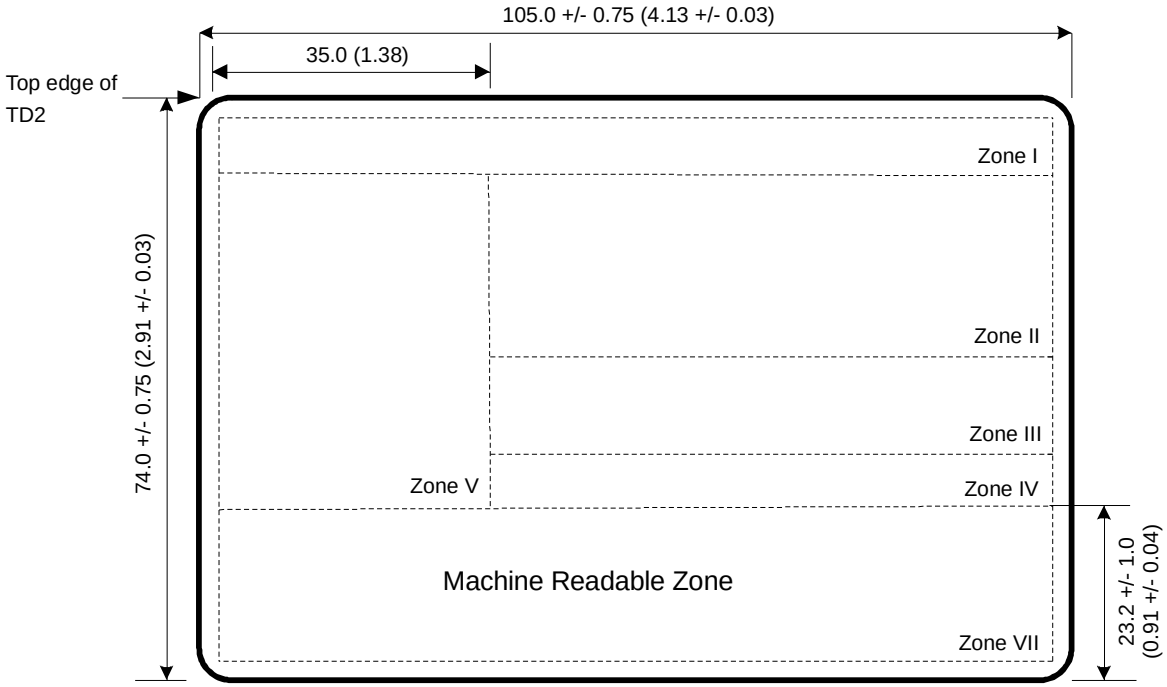


Figure 3. Nominal layout of the Zones on the front side of a TD2 Size MROTD

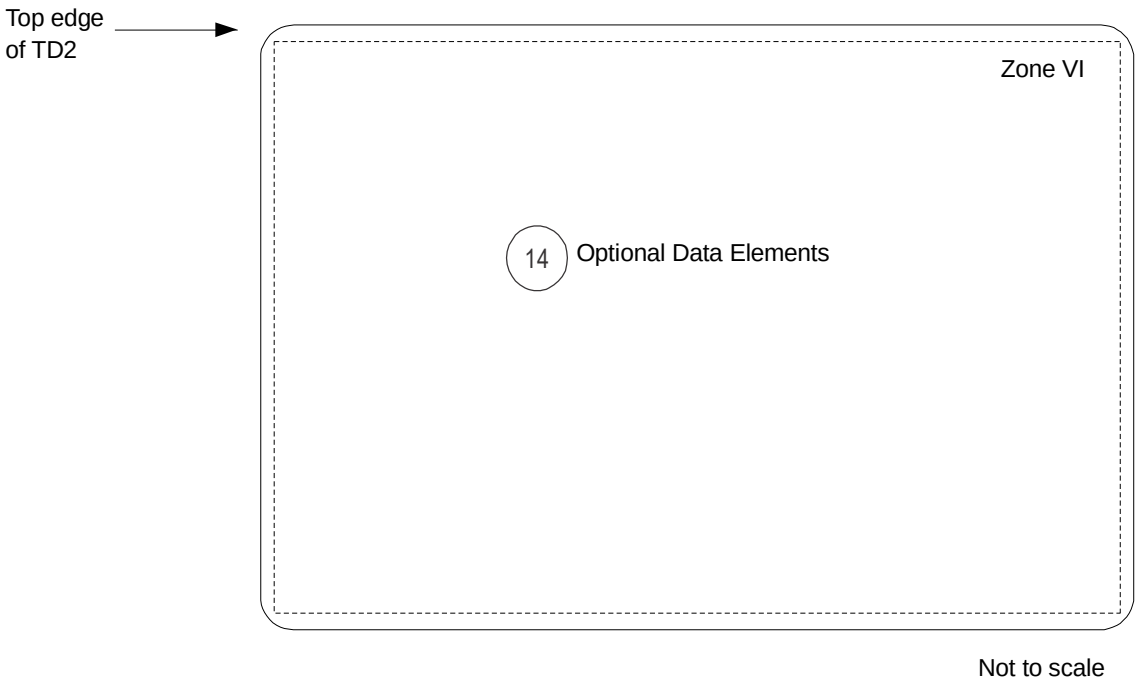


Figure 4. The reverse side of a TD2

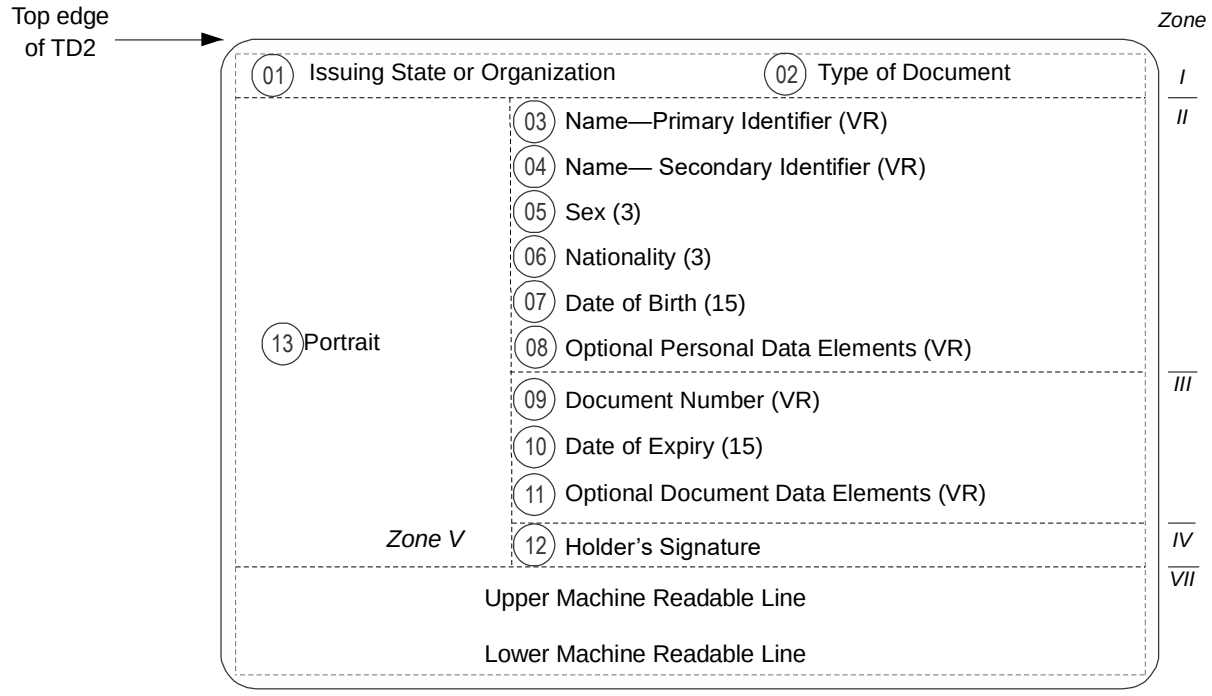


Figure 5. Sequence of data elements on the front side of a TD2

3.1.2 Back of the TD2

Zone VI Optional data elements

3.2 Content and Use of Zones

The data elements to be included in the zones, the preparation of the zones and guidelines for the dimensional layout of zones shall be as described hereunder and illustrated in Figures 4 and 5.

Zones I to V and Zone VII contain mandatory elements which represent the minimum requirements for the TD2. The optional elements in Zones II, III and VI accommodate the diverse requirements of issuing States or organizations, allowing for presentation of additional data, while achieving the desired level of standardization. The location of zones and data elements are set out in Figures 3 through 6. Figures 7 and 8 show some examples for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States or organizations. Examples of a personalized TD2 are shown in Appendix A, Figures 9 to 12.

3.2.1 Mandatory zones

Zone I on the front of the TD2 identifies the issuing State or organization and the document.

Data elements shall appear in a standard sequence in Zones II and III.

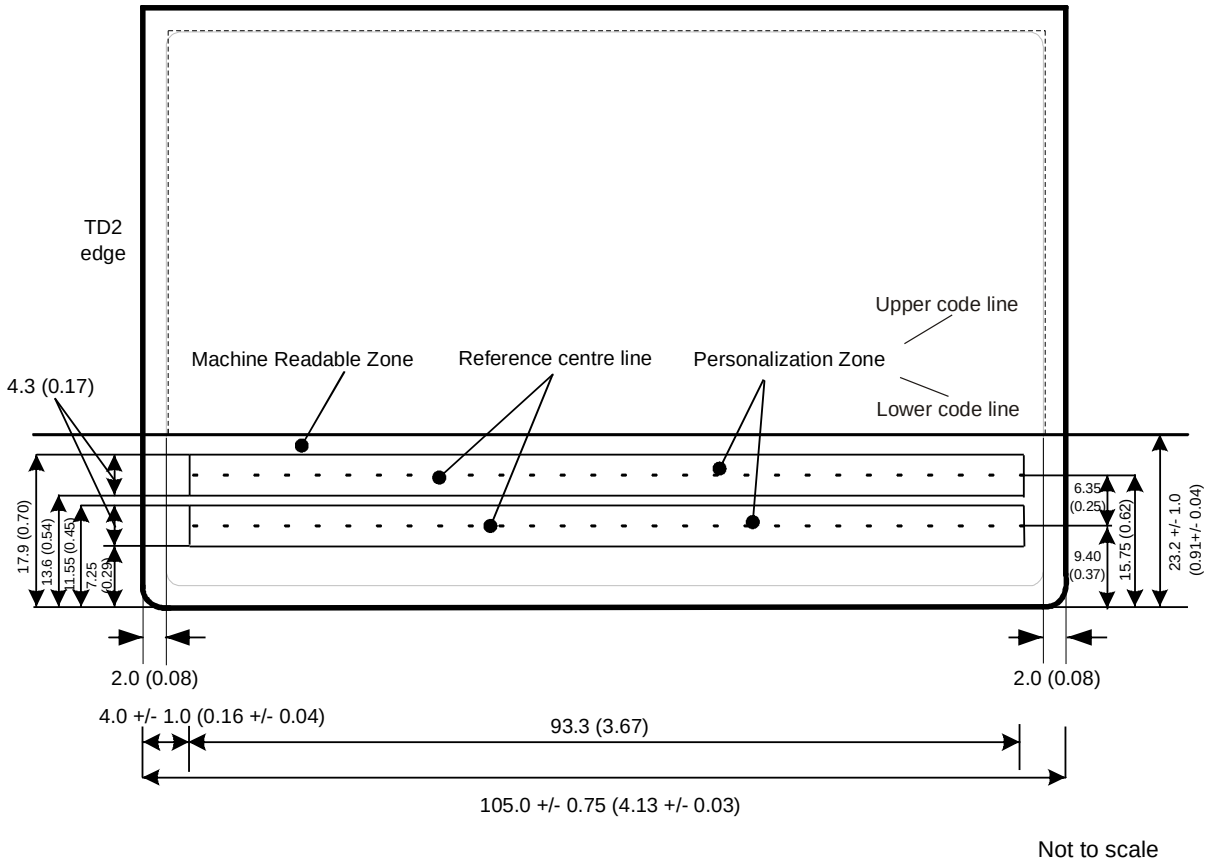


Figure 6. Position and dimensions of Zone VII the Machine Readable Zone

Zones II and III each contain a field in which optional data elements may be included. The optional field in Zone II shall be used for personal data elements and the optional field in Zone III for document-related details. Where an issuing State or organization does not use the optional fields in Zones II and III, there is no need to reserve the space for them on the TD2.

Zone IV contains the holder's signature or usual mark. The issuing State or organization shall decide the acceptability of a holder's usual mark.

Zone V shall contain the personal identification feature(s) which shall include a portrait solely of the holder. At the discretion of the issuing State or organization, the name field in Zone II and the holder's signature or usual mark in Zone IV may overlay Zone V provided this does not hinder recognition of the data in any of the three zones.

The position for the holder's portrait is along the left edge of the front of the TD2, as described in Section 3.3 and illustrated in Figure 3. The size of the portrait is specified in the Data Element Directory (Paragraph 4.1.1.1, Item 13/V).

Zone VII, located on the front of the TD2, shall contain the machine readable data. Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the effective reading zone (ERZ) specified in Doc 9303-3.

All MRZ data elements shall be as defined in the Data Element Directory, paragraph 4.2.2.

3.2.2 Optional data zone

Zone VI, on the back of the MROTD, is an optional zone for use at the discretion of the issuing State or organization. Because the TD2 is a card, Zone VI will always appear, irrespective of whether or not it is used. See Figure 4.

3.3 Dimensional Flexibility of Zones I to V

Zones I to V may be adjusted in size and shape within the overall dimensional specifications of the TD2 to accommodate the diverse requirements of issuing States or organizations. All zones, however, shall be bounded by straight lines, and all angles where straight lines join shall be right angles (i.e. 90 degrees). It is recommended that the zone boundaries not be printed on the TD2. Some examples of flexible positioning of the zones are shown in Figures 7 and 8.

When an issuing State or organization chooses to produce a TD2 that contains a transparent or otherwise unprintable border around the card, this will result in a reduction of the available area within the zones. The full TD2 dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the TD2.

Zone I shall be located along the top edge of the TD2 and extend across the full width of the document. The issuing State or organization may vary the *vertical* dimension of Zone I, as required, but this dimension shall be sufficient to allow legible interpretation of the data elements in the zone and shall not be greater than 11.0 mm (0.43 in).

Zone V shall be located such that its left edge is coincident with the left edge of the TD2. Zone V may vary in size but the portrait image shall not exceed 45 mm x 35 mm (1.77 in x 1.38 in), the maximum dimensions specified in the Data Element Directory.

Zone V may move *vertically* along the left edge of the TD2 and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. The scope for such movement is illustrated in Figure 8.

The upper boundary of Zone II shall be coincident with the lower boundary of Zone I.

When there is a specific requirement for the name field to extend across the TD2, Zone II may extend up to the full width of the TD2. In the event the full dimension is used, Zone II shall overlay a portion of Zone V, as illustrated in Figure 12. In this case, issuing States or organizations shall ensure that data contained in either zone are not obscured.

The lower boundary of Zone II may be positioned at the discretion of the issuing State or organization; examples are shown in Figures 7 and 8. Enough space must be left for Zones III and IV. This boundary does not need to be straight across the longer dimension of the TD2. Figure 7 illustrates a Zone II with the lower boundary on two levels. The flexible design for the Zone II illustrated conforms with the specifications defined above.

Zone III may start at the right vertical boundary of Zone V and may extend, at the discretion of the issuing State or organization, to the right edge of the TD2. Figures 7 and 8 also illustrate some options for a flexible layout of Zone III.

The position of Zone IV is illustrated in Figures 7 and 8 and in the examples shown in Appendix A.

Zone IV may overlay Zone V, as illustrated in Figure 11, although this is not recommended practice. In this case, issuing States or organizations shall ensure that individual details contained in either zone are not obscured.

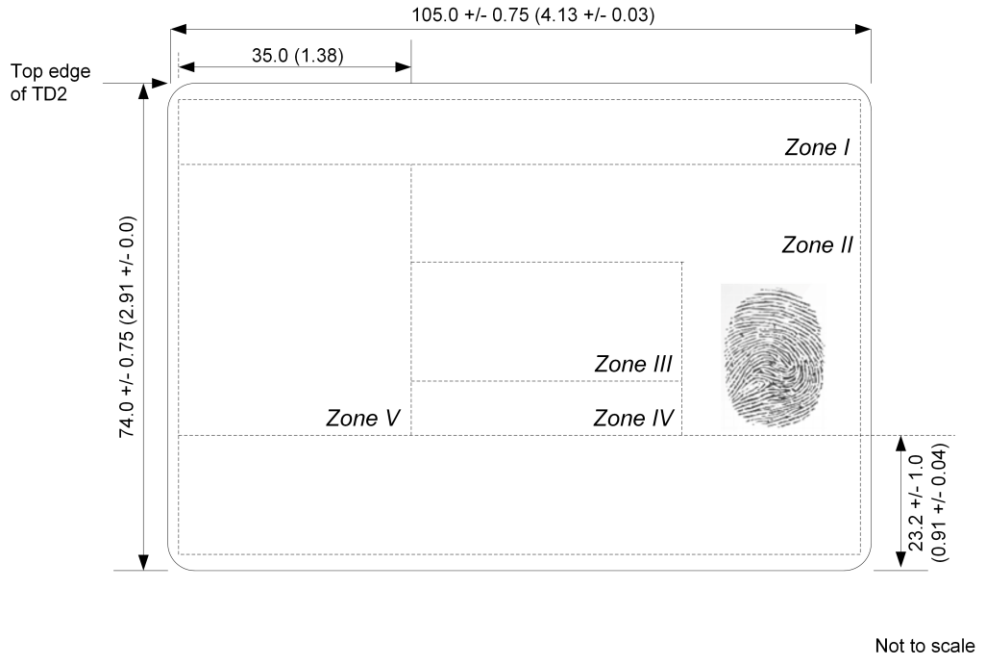


Figure 7. Zones III and IV have been reduced in size to permit the addition of an optional displayed identification feature e.g. a fingerprint, in Zone II

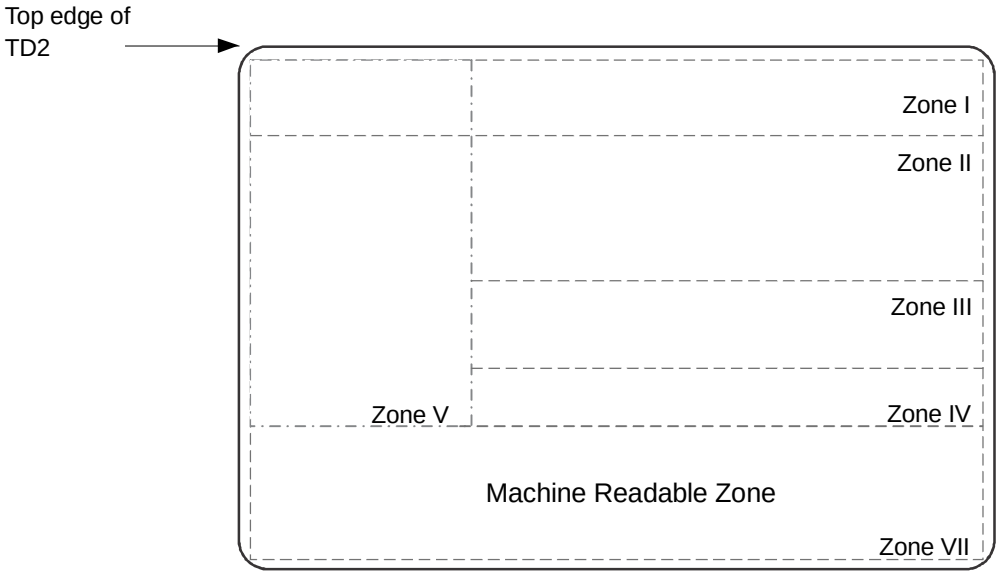


Figure 8. Illustrating the possibility for Zone V to overlay a portion of the Mandatory Header, Zone I

4. CONTENTS OF A TD2 SIZE MROTD

4.1 Visual Inspection Zone (VIZ) (Zones I through VI)

All data in the VIZ shall be clearly legible.

Guidance on the typeface, size and line spacing, the languages and character set, and the field captions to be used in the VIZ may be found in Doc 9303-3.

If any optional field or data element is not used, the data may be spread more evenly in the visual zone of the TD2 consistent with the requirement for sequencing zones and data elements.

4.1.1 Data element directory

4.1.1.1 Visual inspection zone — Data element directory

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
01/I (Mandatory)	Issuing State or organization	The name of the State or organization responsible for issuing the travel document shall be displayed. See Doc 9303-3 for further details.	Variable	Notes a, c, e, h, i.
02/I (Mandatory)	Document	The type or designation of the document. For additional details see Doc 9303-3.	Variable	Notes a, b, c, e, i.
03/04/II (Mandatory)	Name	The full name of the holder, as identified by the issuing State or organization. For additional details see Doc 9303-3.	Variable	Doc 9303-3 Notes a, c, i, l.
03/II (Mandatory)	Primary identifier	Predominant component(s) of the name of the holder as described in Doc 9303-3. In cases where the predominant component(s) of the name of the holder (e.g. where this consists of composite names) cannot be shown in full or in the same order, owing to space limitations of Field(s) 03 and/or 04 or national practice, the most important component(s) (as determined by the State or organization) of the primary identifier shall be inserted.	Variable	Notes a, c, i, l.
04/II (Mandatory)	Secondary identifier	Secondary component(s) of the name of the holder, as described in Doc 9303. The most important component(s) (as determined by the State or organization)	Variable	Notes a, c, i, l.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
		of the secondary identifier of the holder shall be inserted in full, up to the maximum dimensions of the field frame. Other components, where necessary, may be represented by initials. Where the holder's name has only predominant component(s), this data field shall be left blank. The State or organization may optionally utilize the whole zone comprising Fields 03 and 04 as a single field. In such a case the primary identifier shall be placed first, followed by a comma and a space, followed by the secondary identifier.		
05/II (Mandatory)	Sex	Sex of the holder, to be specified by use of the single initial commonly used in the language of the State or organization where the document is issued and, if translation into English, French or Spanish is necessary, followed by an oblique and the capital letter F for female, M for male, or X for unspecified.	3	Notes a, c, f, i, l.
06/II (Mandatory)	Nationality	For details see Doc 9303-3.	Variable	Notes a, h, l.
07/II (Mandatory)	Date of birth	Holder's date of birth as recorded by the issuing State or organization. For unknown dates see Doc 9303-3.	15	Notes a, b, c, i, l.
08/II Optional element in mandatory zone	Optional personal data elements	Optional personal data elements, e.g. personal identification number or fingerprint, at the discretion of the issuing State or organization. If a fingerprint is included in this field, it should be presented as a 1:1 representation of the original. If a date is included, it shall follow the form of presentation described in Doc 9303-3.	Variable	Notes a, b, c, d, g, i.
09/III (Mandatory)	Document number	As given by the issuing State or organization, to uniquely identify the document from all other MRTDs issued by the State or organization. For additional details see Doc 9303-3.	Variable	Notes a, b, c, i, j, l.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
10/III (Mandatory)	Date of expiry	Date of expiry of the document. For additional details see Doc 9303-3.	15	Notes a, b, c, i, l.
11/III Optional element in mandatory zone	Optional document data elements	Optional data elements relating to the document. For additional details see Doc 9303-3.	Variable	Notes a, b, c, d, g, i, j.
12/IV	Holder's signature or usual mark (Mandatory)	Signature or usual mark of the holder. For additional details see Doc 9303-3.		Note g.
13/V	Identification Feature (Mandatory)	This field shall contain a portrait of the holder. The portrait shall not be larger than 45.0 mm x 35.0 mm (1.77 in x 1.38 in) nor smaller than 32.0 mm x 26.0 mm (1.26 in x 1.02 in). The position of the field concerned shall be along the left edge of the front of the TD2. See Doc 9303-3 for additional specifications for the portrait.		Note e.
14/VI	Optional data elements (Optional)	Additional optional data elements at the discretion of the issuing State or organization.		Notes a, b, c, d, g, i.

** Notes can be found in the last portion of sub-section 4.2.2.2.*

4.2 Machine Readable Zone (MRZ) (Zone VII)

4.2.1 Data position, data elements, and print position in the MRZ

4.2.1.1 Data position

Figure 6 shows the nominal dimensions and position of the data in the MRZ.

4.2.1.2 Data elements

The data elements corresponding to specified fields of the VIZ shall be printed, in machine readable form, in the MRZ, beginning with the left most character position in each field in the sequence indicated in the data structure specifications. Details on the data elements to be included in the MRZ are set out in Paragraph 4.2.2. Appendix B, Figure 13 indicates the structure of the MRZ.

4.2.1.3 Print position

The position of the left-hand edge of the first character shall be 4.0 ± 1.0 mm (0.16 ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the OCR lines and a nominal starting position for the first character of each line are shown in Figure 6. The positioning of the characters is indicated by those reference lines and by the printing zones for the two code lines.

4.2.2 Data structure of machine readable data for the TD2

4.2.2.1 Data structure of the upper machine readable line

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 2	02	Document code	Two characters, the first of which shall be A, C or I, shall be used to designate the particular type of document. The second character shall be as specified in Note k.	2	Notes a, b, c, e, k.
3 to 5		Issuing State or organization	The three-letter code specified in Doc 9303-3 shall be used. Spaces shall be replaced by filler characters (<).	3	Notes a, c, e.
6 to 36	03, 04	Name	The name consists of primary and secondary identifiers which shall be separated by two filler characters (<<). Components within the primary or secondary identifiers shall be separated by a single filler character (<). When the name of the document holder has only one part, it shall be placed first in the character positions for the primary identifier, filler characters (<) being used to complete the remaining character positions of the MRZ. For additional details see Doc 9303-3.	31 (Primary identifier(s), secondary identifier(s) and fillers)	Notes a, c, e.
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ. For details on apostrophes, hyphens, commas, etc., see Doc 9303-3.		

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
		Name prefixes and suffixes	For details see Doc 9303-3.		
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 31 characters in total, all permitted name components shall be included in the MRZ, and all unused character positions shall be completed with filler characters (<) repeated up to position 36 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for the name (i.e. 31), they shall be truncated as follows: Characters shall be removed from one or more components of the primary identifier until three character positions are freed and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character position (position 36 in the line, 31st character of the name) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred.		Notes: a, c, e and 4.2.3.

MRZ character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
			Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 36 in the line, 31st character of the name). This indicates that truncation may have occurred. When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 31, characters shall be removed from one or more components of the name until the last character in the name field shall be an alphabetic character.		

** Notes can be found in the last portion of sub-section 4.2.2.2.*

4.2.2.2 Data structure of the lower machine readable line

MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 9	09	Document Number	As given by the issuing State or organization, to uniquely identify the document from all other MRTDs issued by the State or organization. Spaces shall be replaced by filler characters (<).For additional details see Doc 9303-3.	9	Notes a, b, e, j.
10		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Notes b, c, j.
11 to 13	06	Nationality	For details see Doc 9303-3.	3	Notes a, c, e, h.

MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
14 to 19	07	Date of birth	For details see Doc 9303-3.	6	Notes b, c, e.
20		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b.
21	05	Sex	F = female; M = male; < = unspecified.	1	Notes a, c, e, f.
22 to 27	10	Date of expiry	For details see Doc 9303-3.	6	Notes b, e.
28		Check digit	Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b.
29 to 35		Optional data elements	For use of the issuing State or organization. Unused character positions shall be completed with filler characters (<) repeated up to position 35 as required. For additional details see Doc 9303-3.	7	Notes a, b, c, d, e, j.
36		Composite check digit	Composite check digit to verify the data elements of the lower machine readable line. Shall be calculated as specified in Doc 9303-3 and positioned as specified in paragraph 4.2.4.	1	Note b.

* Notes for 4.1.1 and 4.2.2

a) Alphabetic characters (A–Z). National characters may be included in the VIZ. In the MRZ only the characters defined in Doc 9303-3 shall be used.

b) Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ only the numerals 0–9 may be used as defined in Doc 9303-3.

c) Punctuation may be included in the VIZ. In the MRZ only the filler character specified in Doc 9303-3 may be used.

d) Optional data elements may appear in Zone VI.

e) The field caption is not printed on the document.

f) Where an issuing State or organization does not want to identify the sex, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.

g) The use of a caption to identify the field is at the option of the issuing State or organization.

h) In the case of a document issued by the United Nations Organization, or one of its specialized agencies, to a designated official, the appropriate organization code is used in lieu of nationality. See Doc 9303-3.

i) A blank space (or spaces) is included. Blank spaces between words shall count towards the maximum number of characters permitted in the field.

j) The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 1 to 9. They shall be followed by a filler character instead of a check digit to indicate a truncated number. The remaining characters of the document number shall be shown at the beginning of the field reserved for optional data elements (character positions 29 to 35 of the lower machine readable line) followed by a check digit and a filler character.

k) The first character shall be A, C or I. Historically these three characters were chosen for their ease of recognition in the OCR-B character set. The second character shall be at the discretion of the issuing State or organization except that V shall not be used, and C shall not be used after A.

l) The field caption shall be printed on the document.

4.2.3 Truncation of names in the MRZ

The basic rules for writing the name of the holder in the VIZ and the MRZ are contained in Doc 9303-3. Where the name contains more characters than are available in the name field of the MRZ of the TD2, it is necessary to truncate the name. The following methods provide a number of options available for use at the discretion of the issuing State or organization.

4.2.3.1 Truncated names — Secondary identifier truncated

a) One or more name components truncated to initials:

Name: Nilavadhanananda Chayapa Dejthamrong Krasuang
VIZ: NILAVADHANANANDA, CHAYAPA DEJTHAMRONG KRASUANG
MRZ (upper line): I<UTONILAVADHANANANDA<<CHAYAPA<DEJ<K

b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
MRZ (upper line): I<UTONILAVADHANANANDA<<ARN<PET<CHARO

4.2.3.2 Truncated names — Primary identifier truncated

a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): I<UTOBENNELONG<WOOLOOMOOLOO<W<W<<D<P

b) One or more components truncated:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): I<UTOBENNELONG<WOOLOOM<WAR<WARN<<D<P

c) One or more components truncated to a fixed number of characters:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): I<UTOBENNEL<WOOLO<WARRA<WARNA<<DIN<P

4.2.3.3 Names that fit into the maximum positions available within in the name field, indicating possible truncation by the letter in the last position, but which are not truncated

Name: Jonathoon Alec Papandropoulous
VIZ: PAPANDROPOULOUS, JONATHOON ALEC
MRZ (upper line): I<UTOPAPANDROPOULOUS<<JONATHOON<ALEC

Note.— Even though there is an alphabetic character in the 36th character position of this TD2 lower machine readable line, this name has not been truncated, but it must be assumed that it has been truncated.

4.2.3.4 Multiple Name components including hyphens

Name: Martin Van Der Muellen
VIZ: VAN DER MUELLEN, MARTIN
MRZ (upper): I<UTOVAN<DER<MUELLEN<<MARTIN<<<<<<<<

Name: Huda Muhammad Jawad Al-Basri
VIZ: AL-BASRI, HUDA MUHAMMAD JAWAD
MRZ (upper): I<UTOAL<BASRI<<HUDA<MUHAMMAD<JAWAD<<

Name: Jose Ramon Vilarchao Fernandez
VIZ: VILARCHAO FERNANDEZ, JOSE RAMON
MRZ (upper): I<UTOVILARCHAO<FERNANDEZ<<JOSE<RAMON

4.2.3.5 No secondary identifier

Name: Arkfreith
VIZ: ARKFREITH
MRZ (upper line): I<UTOARKFREITH<<<<<<<<<<<<<<<<<<<<<

Name: Satriya Sudarpa
VIZ: SATRIYA SUDARPA
MRZ (upper line): I<UTOSATRIYA<SUDARPA<<<<<<<<<<<<<<<

4.2.4 Check digits in the MRZ

The method of calculating check digits is given in Doc 9303-3. For the TD2, the data structure of the machine readable lines in Paragraph 4.2.2 provides for the inclusion of four check digits as follows:

Check digit	*Character positions (lower MRZ line) used to calculate check digit*	*Check digit position (lower MRZ line)*
Document number check digit	1 – 9	10
Date of birth check digit	14 – 19	20
Date of expiry check digit	22 – 27	28
Composite check digit	1 – 10, 14 – 20, 22 – 35 (lower line) *Note.— Positions 11 – 13 and position 21 (lower line) are excluded in calculating the composite check digit.*	36

4.3 Representation of the Issuing State or Organization and Nationality of the Holder in the MRZ and the VIZ

The use of the three-letter codes listed in Doc 9303-3 is mandatory in the MRZ. In the VIZ, the name of the issuing State or organization should appear in full; the holder's nationality in the VIZ may either appear in full or in the form of the three-letter code. Specific locations are defined in the following table.

	Zone	*Field no.*	*Character position no.*	*Number of character positions*
Issuing State or organization	VIZ MRZ (upper line)	01	– 3 – 5	Variable 3
Holder's nationality	VIZ MRZ (lower line)	06	– 11 – 13	Variable 3

5. REFERENCES (NORMATIVE)

ISO/IEC 7810 ISO/IEC 7810:2003, Identification cards — Physical characteristics

ISO 1073-2 ISO 1073-2:1976 — Alphanumeric character sets for optical recognition CS Part 2: Character set OCR-B — Shapes and dimensions of the printed image

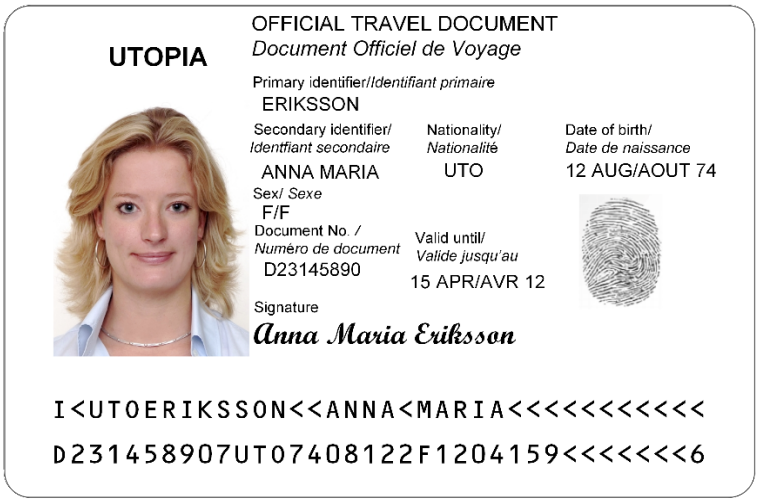
— — — — — — — —

Appendix A to Part 6

EXAMPLES OF A PERSONALIZED TD2 SIZE MROTD (INFORMATIVE)

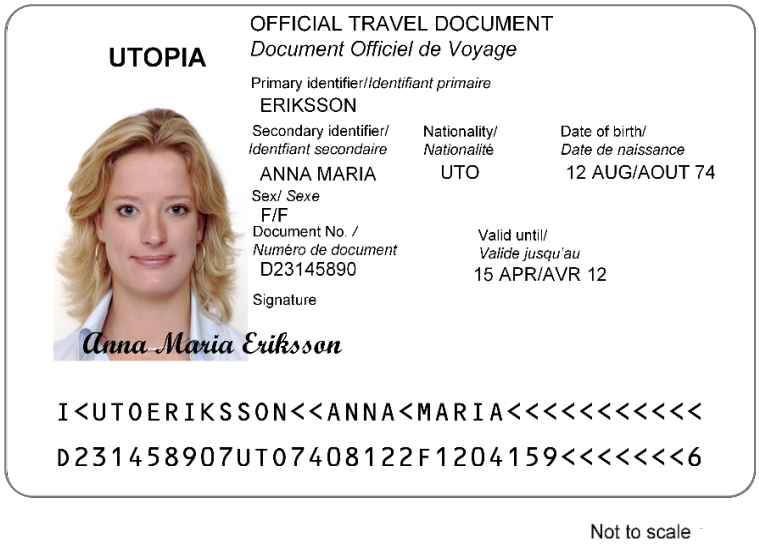
Not to scale

Figure 9. Typical layout of a TD2 Size MROTD



Not to scale

Figure 10. Flexible layout in which Zone II has been enlarged to accommodate an optional displayed fingerprint



Not to scale

Figure 11. Flexible layout in which Zone IV, the signature, overlays the portrait, Zone V

Not to scale

Figure 12. Flexible layout in which Zone II has been extended to the left to overlap Zone V, the portrait. Zone III has been extended upwards, beside and to the right of Zone I, to accommodate the Document Number

— — — — — — — —

Appendix B to Part 6

CONSTRUCTION OF THE MACHINE READABLE ZONE OF A TD2 SIZE MROTD (INFORMATIVE)

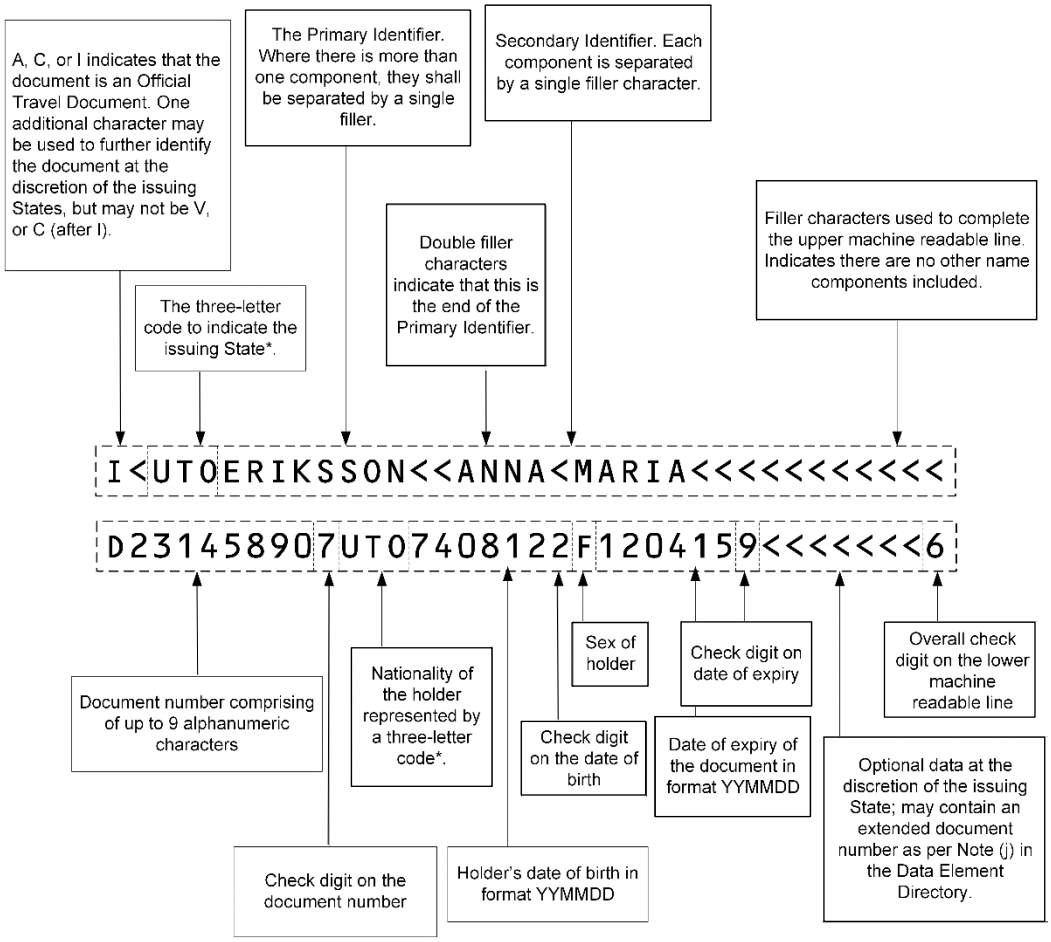


Figure 13. Construction of the MRZ data on a TD2 Size MROTD

* Three-letter codes are given in Doc 9303-3.

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2020

Part 7: Machine Readable Visas

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 7 — *Machine Readable Visas*
ISBN 978-92-9249-796-5

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

Page

1. SCOPE

Part 7 defines the specifications for machine readable visas (MRV) which allow compatibility and global interchange using both visual (eye readable) and machine readable means. The specifications lay down standards for visas which can, where issued by a State and accepted by a receiving State, be used for travel purposes. The MRV shall, as a minimum, contain the data specified herein in a form that is legible both visually and by optical character recognition methods, as presented herein. Part 7 contains specifications for both Format-A and Format-B types of visas.

Part 7 shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 2 — *Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*;
- Part 3 — *Specifications common to all MRTDs*.
- Part 13 — *Visible Digital Seals for non-electronic documents*

2. TECHNICAL SPECIFICATIONS FOR FORMAT-A MACHINE READABLE VISAS (MRV-A)

This section defines those specifications which are unique to Format-A machine readable visas (MRV- A) and are necessary for global interoperability. Specifications are included for the discretionary expansion of the machine readable data capacity of the MRV beyond that defined for global interoperability. The Format-A visa (MRV-A) is suitable for use by States that wish to have maximum space available to accommodate their data requirements and that do not need to maintain a clear area on the passport visa page adjacent to the visa.

2.1 Dimensions and Placement of the MRV-A

The dimensions and placement of the MRV-A shall be as follows:

MRV-A nominal dimensions. The nominal dimensions of the MRV-A shall be as follows:

80.0 mm × 120.0 mm (3.15 in × 4.72 in)

MRV-A margins. The dimensional specifications refer to the outer limits of the MRV-A. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data.

MRV-A edge tolerances. The edges of the MRV-A shall be within the area circumscribed by the concentric rectangles as illustrated in Figure 1.

Inner rectangle: 79.0 mm × 119.0 mm (3.11 in × 4.69 in)
Outer rectangle: 81.0 mm × 121.0 mm (3.19 in × 4.76 in)

MRV-A thickness. If the visa is issued as a label, the increase in thickness once the label is attached to the passport visa page shall not exceed 0.19 mm (0.0075 in). The thickness of the area within the machine readable zone (MRZ) shall not vary by more than 0.05 mm (0.002 in). If a protective laminate is used, it is recommended that its thickness not exceed

0.15 mm (0.006 in).

General note.— The decimal notation used in these specifications conforms to ICAO practice. This differs from ISO practice where a decimal point (.) in imperial measurements and a comma (,) in metric measurements are used.

Placement of the MRV-A. The MRV-A shall be positioned as follows:

The MRV-A shall be located on the passport visa page such that the MRZ is coincident with and parallel to the outside edge (reference edge) of the passport visa page, and the left edge of the MRV-A is coincident with and parallel to the left edge of the passport visa page as defined in Appendix C, Section C.1.

The MRZ shall be located such that the two OCR lines contained therein are within the Effective Reading Zone (ERZ) as defined in Doc 9303-3.

Only one MRV-A shall be located on a passport visa page (see Appendix C, Section C.1).

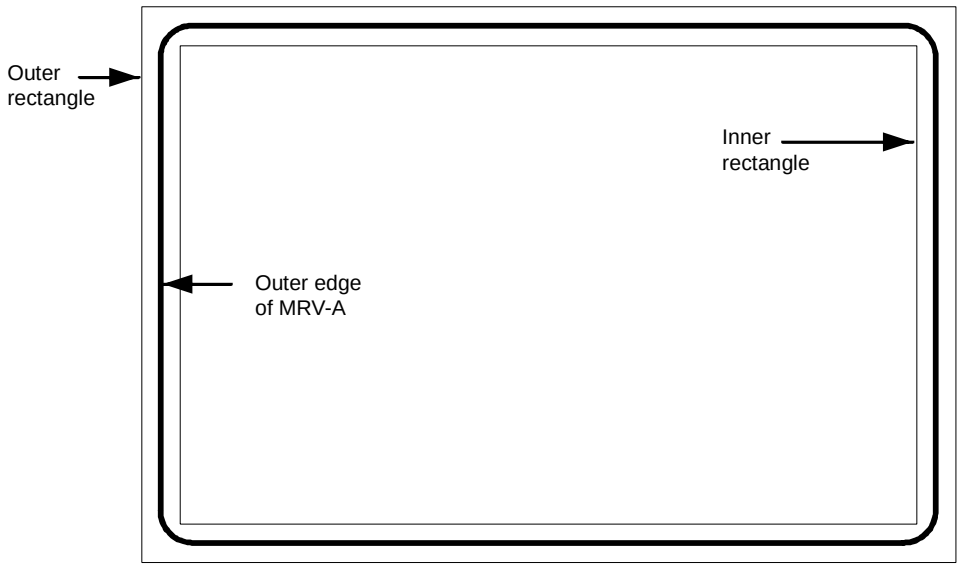


Figure 1. MRV-A dimensional illustration

3. GENERAL LAYOUT OF THE MRV-A

The MRV-A follows a standardized layout to facilitate reading of data globally, by visual and machine readable means, to accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements.

The standard layout incorporates space for a portrait of the holder and other identification feature(s). The inclusion of a portrait on a visa is strongly recommended in the interests of security, but States who are not yet able to apply portraits may fill this space with, for example, a national crest.

3.1 MRV-A Zones

An MRV-A is divided into six zones as follows:

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Signature (original or reproduction) or authentication
Zone V	Mandatory zone for identification feature (feature optional)
Zone VII	Mandatory machine readable zone (MRZ)

Note 1.— The signature in Zone IV of a visa is that of an issuing officer, not of the document holder. The signature may be replaced or accompanied by an official stamp.

Note 2.— To facilitate inspection of visas at border control, the layout of the visa presents Zone III above Zone II.

Note 3.— Zone VI is not available on an MRV issued in the form of a label.

Note 4.— Zones I to V constitute the Visual Inspection Zone (VIZ).

Zones I and VII are mandatory. Certain data in Zones II and III are also mandatory. The mandatory components of these four Zones represent the minimum data requirements for an MRV-A. The optional data elements in Zones II, III and V and in optional Zone IV may be utilized to accommodate the diverse requirements of States, while achieving the desired level of standardization. The data elements which may be included in the various zones and their order are set out in Section 4.4. Section 0 also illustrates the dimensional specifications and tolerances for the layout of the MRV-A and the technical specifications for the printing of data elements within the zones, as well as the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States. Examples of personalized MRV-As are shown in Appendix A, Section A.1. Appendix B, Section B.1 illustrates the format for the presentation of the machine readable data in Zone VII.

3.2 Content, Use and Dimensional Flexibility of Zones

The data elements to be included in the zones, the treatment of the zones and guidelines for the dimensional layout of zones shall be as described hereunder.

Zone I identifies the issuing State and the type of document. These elements are mandatory. The order of the data elements in this zone is left to the discretion of the issuing State.

To facilitate the checking of visas by airline personnel and control authorities, the essential details of the visa document shall be entered in a standard sequence in Zone III while essential personal details of the holder shall be entered in a standard sequence in Zone II. On a visa, Zone III appears above Zone II.

Zone IV provides space for an optional signature or authentication. This is normally the signature of the issuing officer or an official stamp. The application of an official stamp elsewhere on the document is not precluded except that it must not intrude into the MRZ or affect the legibility of entered data.

Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the ERZ specified in Doc 9303-3, thus allowing a single reader to be used for all types and sizes of MRTDs.

All MRZ data elements are mandatory and shall be shown as defined in Section 04.2 even though an issuing State may choose not to include a specific MRZ data element in the VIZ.

3.3 Dimensional Flexibility of Zones I to V

Zones I to V may be adjusted in size and shape within the overall dimensional specifications of the MRV-A to accommodate the diverse requirements of issuing States. All zones, however, shall be bounded by straight lines, and all angles where straight lines join shall be right angles (i.e. 90 degrees). It is recommended that the zone boundaries not be printed on the MRV-A. The nominal position of the zones is shown in Section 4.4, Figure 4.

When an issuing State chooses to produce an MRV-A as a securely attached card containing a transparent or otherwise unprintable border around the card, the available area within the zones will be reduced. The full MRV-A dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the MRV-A.

Zone I shall be adjacent and parallel to the top edge of the MRV-A and extend across the full 120.0 mm ± 1.0 mm (4.72 in ± 0.04 in) dimension. The issuing State may vary the *vertical* dimension of Zone I, as required, but this dimension shall be sufficient to allow legibility of the data elements in the zone, and the height shall not be greater than 12.0 mm (0.47 in) as defined in Section 4.4, Figure 4.

Zone V shall be located such that its left edge is coincident with the left edge of the MRV-A, as defined in Section 4.4, Figure 4. Zone V may vary in size but any variation from the nominal dimensions shall not exceed the tolerances specified in Section 4.4, Figure 4.

Zone V may move *vertically* along the left edge of the MRV-A and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. Zone V may, as a result, have its *lower external boundary* coincident with the top edge of the MRZ of the MRV-A and its *upper external boundary* coincident with the top edge of the MRV-A.

The upper boundary of Zone III shall be coincident with the lower boundary of Zone I.

Zone III may extend to the full width of that portion of the MRV-A to the right of Zone V.

The lower boundary of Zone III (see Section 4.4, Figure 4) may be positioned at the discretion of the issuing State. Enough space shall be left for Zone II and Zone IV (when used) below the boundary.

Normally, the upper boundary of Zone II should be coincident with the lower boundary of Zone III. The boundary does not have to be straight across the 120.0 mm ± 1.0 mm (4.72 in ± 0.04 in) dimension of the visa. Zone II may also overlay a portion of Zone V for the MRV-A, if required. When this occurs, issuing States shall ensure that data contained in either zone are not obscured. See Appendix A – 0Figure 14.

Zone IV, when included on the MRV-A, shall be entered on the right hand side of the visa immediately above but not intruding into the MRZ. See Section 4.4, Figure 5.

4. DETAILED LAYOUT OF MRV-A

4.1 Visual Inspection Zone (VIZ) (Zones I-V)

All data in the VIZ shall be clearly legible.

Print spacing. The design of the MRV-A in Zones II and III is based on a vertical line spacing of a maximum of 8 lines per 25.4 mm (1.0 in) and a horizontal printing density of a maximum of 15 characters per 25.4 mm (1.0 in). This spacing has been chosen as the smallest in which information is clear and legible. If any optional field or data element is not used, the entered data may be spread out in the VIZ of the MRV-A consistent with the requirement for sequencing zones and data elements. This horizontal printing density and the font and the vertical line spacing may be adjusted at the discretion of each State, provided that in the VIZ all data shall be printed in a size such that they can be easily read and assimilated by a person with normal eyesight. Typical configurations are shown in Appendix A. Zone VII, the mandatory MRZ, shall be printed with a line spacing as defined in Section 4.4, Figure 3, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

4.1.1 Data element directory

4.1.1.1 Visual inspection zone — Data element directory

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
01/I Mandatory	Issuing State	The State responsible for issuing the MRV-A. This shall be personalized, the type font being selected at the discretion of the issuing State. For transliteration rules, refer to Doc 9303-3.	Variable	Notes a, c, d, e, i.
02/I Mandatory	Document	The word or words in the language of the issuing State for the document (visa or other appropriate document) which confers on the holder that State's authority to travel to a port of entry in its territory.	Variable	Notes a, c, d, e, i.
03/III Mandatory	Place of issue	Post/location (usually a city) where the MRV-A is issued. A translation of the name into one or more languages, one of which should be English, French or Spanish, shall be given when the translated name is more familiar to the international community.	15	Notes a, b, c, i, k.
04/III Mandatory	Valid from (date)	In most cases this will be the date of issue of the MRV-A and indicates the first date from which the MRV-A can be used to seek entry. For some States the date of issue and the date the visa becomes valid	8	Notes a, b, c, i, k.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
		may differ. In such cases the latter shall be indicated in this field and the date of issue may be shown in Field 09 (see below). For date format, refer to Doc 9303-3.		
05/III Mandatory	Valid until (date)	In most cases this will be the date of expiry of the MRV-A and indicates the last day on which the MRV-A can be used to seek entry. For some States this will be the date by or on which the holder should have left the country concerned. For date format, refer to Doc 9303-3.	8	Notes a, b, c, i, k.
06/III Mandatory	Number of entries	The number of entries for which the visa is valid.	8	Notes a, b, c, i, k.
07/III Mandatory	Document number	The number given to the visa by the issuing State.	13	Notes a, b, c, i, j, k.
08/III Mandatory	Type/class/ category	This field shall include one or more of the following elements: • the issuing State's indication of the type and/or class of visa granted in accordance with the law/practice of that State; • the broad categorization of the type of visa granted, e.g. visitor/resident/ temporary resident/student/diplomat, etc., in accordance with the law/practice of the issuing State; • any limitations on the territorial validity of the visa.	46	Notes a, b, c, i, k.
09/III Optional	Additional information	This field may include necessary endorsements as to entitlements which attach to the visa. The issuing State may also use this field to include a) the maximum authorized duration of stay; b) conditions related to the granting of the visa; c) date of issue if different from "Valid from" date; and d) record of any fees paid.		Note g.
10,11/II	Name	See Doc 9303-3.	Variable	Notes a, c, i.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
Mandatory				
10/II Mandatory	Primary identifier	See Doc 9303-3.	Variable	Notes a, c, i, k.
11/II Optional	Secondary identifier	See Doc 9303-3.	Variable	Notes a, c, i.
12/II Optional	Passport number	The number of the passport or other travel document in which the MRV-A is placed.	Variable	Notes a, b, c, g, i, j.
13/II Optional	Sex	Sex of MRV-A holder, when included, is to be specified by use of the single initial commonly used in the language of the State of issue. If translation into English, French or Spanish is necessary, followed by an oblique and the capital letter F for female, M for male, or X for unspecified.	3	Note a, f, g.
14/II Optional	Date of birth	See Doc 9303-3.	9	Notes a, b, c, k.
15/II Optional	Nationality	See Doc 9303-3.	Variable	Notes a, h, k.
16/IV Optional	Signature or other authorization	An authorization which may be the signature of an issuing official and/or an official stamp.		
17/V Mandatory	Identification feature	This field shall be entered on the document and should contain a portrait of the holder. If included, the portrait shall have a size of 36.0 ± 4.0 mm × 29.0 ± 3.0 mm (1.42 ± 0.16 in × 1.14 ± 0.12 in) . If a State does not place an identification feature in this field, a national symbol or logo may be inserted instead. See Doc 9303-3 –- Section 3.9 for additional specifications for the portrait.		

* Notes can be found in 4.2.

4.2 Machine Readable Zone (MRZ) (Mandatory Zone VII)

4.2.1 MRZ position, data elements, print specifications and print position in the MRZ

4.2.1.1 MRZ position

The MRZ is located at the bottom of the MRV-A. Section 4.4, Figure 3, shows the nominal position of the data in the MRZ.

4.2.1.2 Data elements

The data elements corresponding to Fields 01, 05, 10, 11, and 13 to 15 of the VIZ are mandatory in the MRZ and shall be printed in machine readable form in the MRZ, beginning with the leftmost character position in each field in the sequence indicated in the data structure specifications shown below. Appendix B, Section B.1, indicates the structure of the MRZ.

4.2.1.3 Print specifications

Machine readable data shall be printed in OCR-B type font, size 1, constant stroke width, as specified in Doc 9303-3. The MRZ shall be printed with the line spacing as defined in Section 4.4, Figure 3, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

4.2.1.4 Print position

The position of the left-hand edge of the first character shall be 4.0 mm ± 1.0 mm (0.16 in ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the two OCR lines and a nominal starting position for the first character of each line are shown in Section 4.4, Figure 3. The positioning of the characters is indicated by those reference lines and by the printing zones of the two code lines in 0 Section 4.4, Figure 3.

4.2.2 Data Structure of Machine Readable Data for the MRV-A

4.2.2.1 Data structure of the upper machine readable line

MRZ field character positions (line 1)	*Field no in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 2		Type of document	Capital letter V to designate a machine readable visa. One additional character may be used, at the discretion of the issuing State, to designate a particular type of visa. If the second character position is not used for this purpose, it shall be filled by the filler character (<).	2	Notes a, b, c, e.
3 to 5	1	Issuing State	See Doc 9303-3.	3	Notes a, c, e.

MRZ field character positions (line 1)	*Field no in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
6 to 44	10, 11	Name	See Doc 9303-3.	39	Notes a, c, e.
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ.		Doc 9303-3.
		Apostrophes in the name	Components of the primary or secondary identifiers separated by apostrophes shall be combined, and no filler character (<) shall be inserted. Example: VIZ: D'ARTAGNAN MRZ: `DARTAGNAN`		Doc 9303-3.
		Hyphens in the name	Hyphens (-) in the name shall be converted to the filler character (<) (i.e. hyphenated names shall be represented as separate components). Example: VIZ: MARIE-ELISE MRZ: `MARIE<ELISE`		Doc 9303-3.
		Commas	When a comma is used in the VIZ to separate the primary and secondary identifiers, the comma shall be omitted in the MRZ and the primary and secondary identifiers shall be separated by two filler characters (<<). When a comma is used in the VIZ to separate two name components, it shall be represented in the MRZ by a single filler character (<).		Doc 9303-3.
		Name suffixes	Name suffixes (e.g. Jr., Sr., II or III) shall not be included in the MRZ except as permitted by Doc 9303–3 as components of the secondary identifier.		Doc 9303-3.
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 39 characters in total, all name components shall be included in the MRZ and all unused character		

MRZ field character positions (line 1)	*Field no in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
			positions shall be completed with filler characters (<) repeated up to position 44 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 39), they shall be truncated as follows: Characters shall be removed from one or more components of the primary identifier until three character positions are freed, and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 44) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred. Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 44). This indicates that truncation may have occurred. When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 39, characters shall be removed from one or more components of the name until the last character in the name field is an alphabetic character.		Doc 9303-3, Note a.

4.2.2.2 Data structure of the lower machine readable line

MRZ character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 9	07 or 13	Passport or document number	At the discretion of the issuing State, either the passport number or the visa number shall be used in this field; however, the latter option can only be exercised where the visa number has 9 characters or fewer. Any special characters or spaces in the number shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 9 as required.	9	Notes a, b, c, e, j.
10		Check digit	See Doc 9303-3.	1	Notes b, e.
11 to 13	16	Nationality	See Doc 9303-3.	3	Notes a, c, e, h.
14 to 19	15	Date of birth	See Doc 9303-3.	6	Notes b, c, e.
20		Check digit	See Doc 9303-3.	1	Note b.
21	14	Sex	F = Female; M = Male; < = non-specified.	1	Notes a, c, f, g.
22 to 27	5	Valid until (date)	In most cases this will be the date of expiry of the MRV-A and indicates the last day on which the MRV-A can be used to seek entry. For some States this will be the date by or on which the holder should have left.	6	Doc 9303-3; Notes b, e.
28		Check digit	See Doc 9303-3.	1	Note b.
29 to 44		Optional data elements	For optional use of the issuing State. Unused character positions shall be completed with the filler character (<) repeated up to position 44 as required.	16	Notes a, b, c, e.

* Notes:

a) Alphabetic characters (A–Z and a-z). National characters may be used in the VIZ. In the MRZ, only those characters specified in Doc 9303-3 shall be used.

b) Numeric characters (0–9). National numerals may be additionally included in the VIZ. In the MRZ, only the numerals 0–9 may be used as defined in Doc 9303-3.

c) Punctuation may be included in the VIZ. In the MRZ, only the filler character specified in Doc 9303-3 shall be used.

d) The lengths of fields 01 and 02 are undefined, depending on type font and limits set by MRV-A size and position of other fields.

e) The field caption is not printed on the document.

f) Where an issuing State or organization does not want to identify the sex, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.

g) The use of a caption to identify a field is at the option of the issuing State.

h) United Nations Laissez-passer are issued to officials of the United Nations Organization under the terms of the *Convention on the Privileges and Immunities of the United Nations* of 13 February 1946 and to officials of the Specialized Agencies of the United Nations under the terms of the *Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations* of 21 November 1947. In the case of visas entered in the United Nations Laissez-passer, in keeping with the international character of United Nations officials, nationality shall not be shown. Instead the appropriate code shall be entered in accordance with Doc 9303-3.

i) The number of characters (in the field length) includes any blank spaces.

j) The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 1 to 9.

k) The field caption shall be printed on the document.

4.2.3 Examples of Names of the Holder in the MRZ

Note.— In the following examples, the document is assumed to be a visa issued by the State of Utopia. The first five characters of the upper machine readable line are coded "V<UTO".

a) Usual representation:

Name: Anna Maria Eriksson
VIZ: ERIKSSON, ANNA MARIA
MRZ (upper line): `V<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<`

b) Central primary identifier:

Name: Deborah Heng Ming Lo
VIZ: HENG, DEBORAH MING LO
MRZ (upper line): `V<UTOHENG<<DEBORAH<MING<LO<<<<<<<<<<<<<<<<<<`

c) Hyphen as part of the name:

Name: Susie Margaret Smith-Jones
VIZ: SMITH-JONES, SUSIE MARGARET
MRZ (upper line): `V<UTOSMITH<JONES<<SUSIE<MARGARET<<<<<<<<<<<<`

d) Apostrophe as part of the name:

Name: Enya Siobhan O'Connor
VIZ: O'CONNOR, ENYA SIOBHAN
MRZ (upper line): `V<UTOOCONNOR<<ENYA<SIOBHAN<<<<<<<<<<<<<<<<<<`

e) Multiple name components:

Name: Martin Van Der Muellen
VIZ: VAN DER MUELLEN, MARTIN
MRZ (upper line): `V<UTOVAN<DER<MUELLEN<<MARTIN<<<<<<<<<<<<<<<<`

f) No secondary identifier:

Name: Arkfreith
VIZ: ARKFREITH
MRZ (upper line): `V<UTOARKFREITH<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<`

4.2.3.1 Truncated names — Secondary identifier truncated

a) One or more name components truncated to initials:

Name: Nilavadhanananda Chayapa Dejthamrong Krasuang
VIZ: NILAVADHANANANDA, CHAYAPA DEJTHAMRONG KRASUANG
MRZ (upper line): `V<UTONILAVADHANANANDA<<CHAYAPA<DEJTHAMRONG<K`

b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
MRZ (upper line): `V<UTONILAVADHANANANDA<<ARNPOL<PETCH<CHARONGU`

4.2.3.2 Truncated names — Primary identifier truncated

a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): `V<UTOBENNELONG<WOOLOOMOOLOO<WARRANDYTE<W<<DI`

b) One or more components truncated:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): `V<UTOBENNELONG<WOOLOOM<WARRAND<WARNAM<<DINGO`

c) One or more components truncated to a fixed number of characters:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): V<UTOBENNEL<WOOLOO<WARRAN<WARNAM<<DINGO<POTO

4.2.3.3 Names that just fit, indicating possible truncation by letter in the last position of the name field, but which are not truncated

Name: Jonathon Warren Trevor Papandropoulous
VIZ: PAPANDROPOULOUS, JONATHON WARREN TREVOR
MRZ (upper line): V<UTOPAPANDROPOULOUS<<JONATHON<WARREN<TREVOR

Note.— Even though there is an alphabetic character in the 44th character position of this MRV-A upper machine readable line, this name has not been truncated but it shall be assumed that it has been truncated.

4.3 Portrait

Portrait. For the MRV-A, a portrait should be inserted in the rectangular area defined as Zone V. Such portrait, if included, shall represent only the holder of the MRV-A.

Portrait edges. The portrait may have irregular edges. When a digitally printed reproduction is used, the background of the portrait may be dropped out in order to provide protection against forgery or substitution.

Zone V without an identification feature. A standard default image, such as a national symbol, crest or wording, should be selected and used in Zone V when an identification feature is not included.

4.4 MRV-A Diagrams

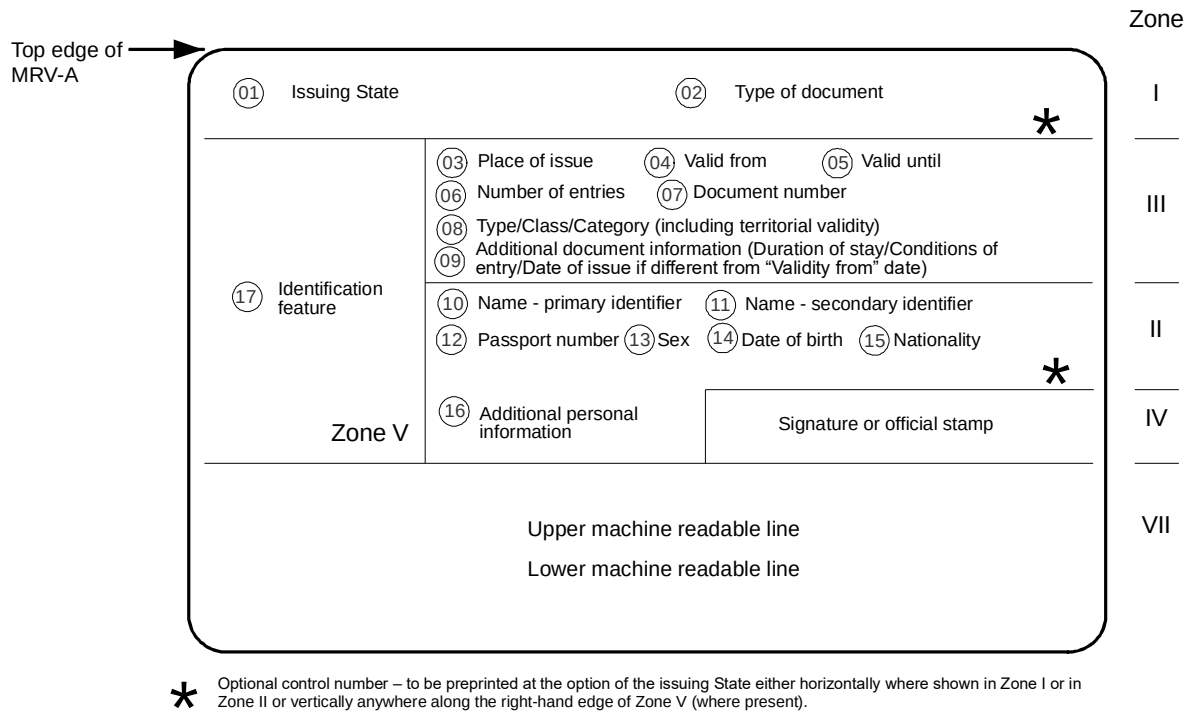


Figure 2. Location of data elements on an MRV-A

Note 1.— VIZ based on maximum printing density of 8 lines per 25.4 mm (1.0 in) and horizontal printing density of 15 characters per 25.4 mm (1.0 in).

Note 2.— MRZ based on horizontal printing of 10 characters per 25.4 mm (1.0 in).

Note 3.— ◯ = field numbers.

Note 4.— The borderlines of the zones are not printed on the actual visa.

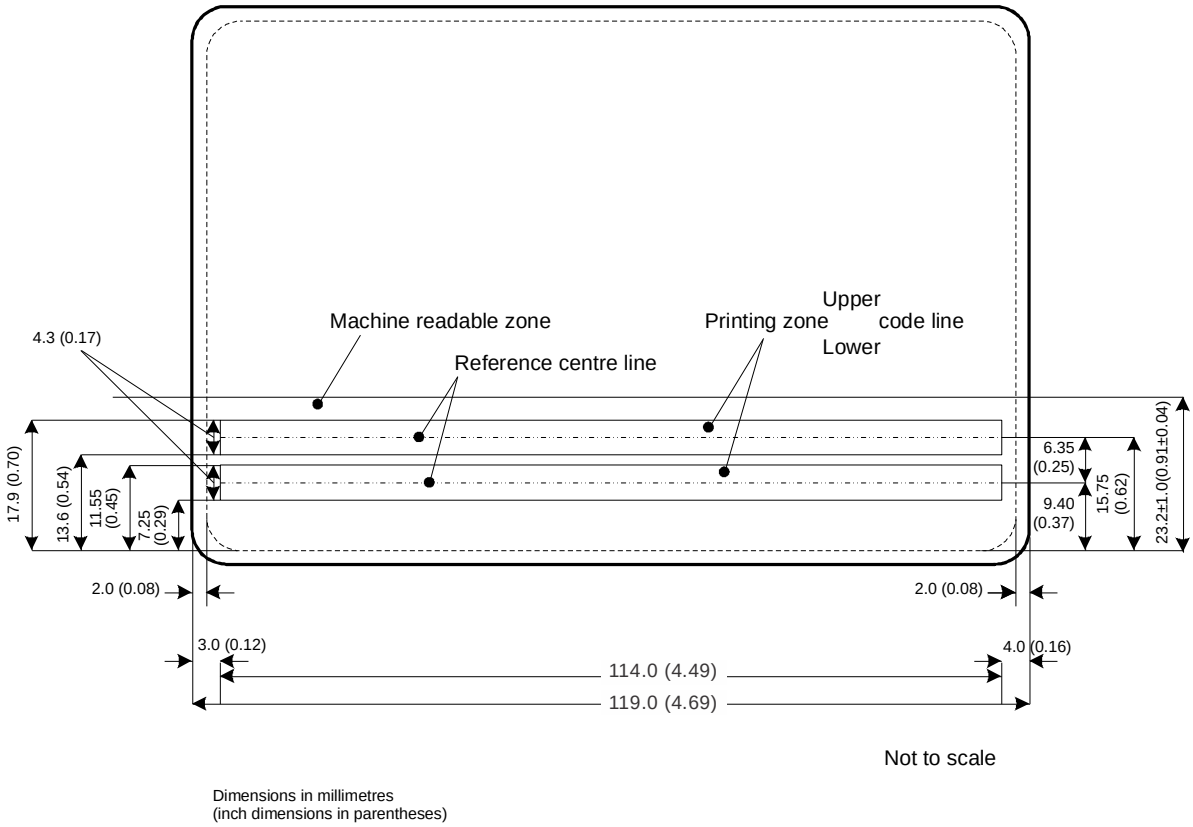


Figure 3. Schematic diagram of the Machine Readable Zone of an MRV-A

Note.— For illustration purposes, the smallest option for the 120.0 mm (4.72 in) dimension of the MRV-A and the smallest option for the left-hand margin in the MRZ have been selected.

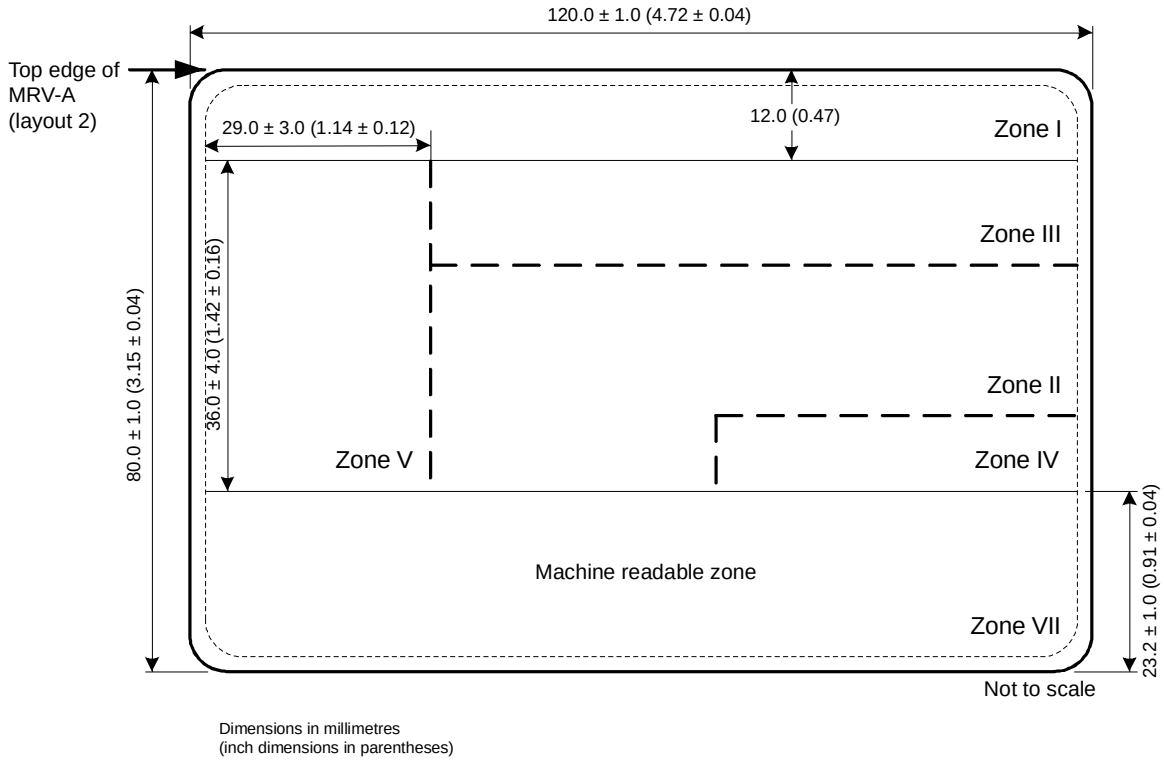


Figure 4. Nominal positioning of zones on an MRV-A

This diagram should be considered in conjunction with 0. It assumes that all the available space for data in the VIZ is used. The line spacing in the VIZ is the closest permitted at 8 lines per 25.4 mm (1.0 in). If an issuing State requires less information, the line spacing can be increased to print fewer lines in the VIZ.

Dotted lines indicate zone boundaries whose positions are not fixed, enabling issuing States flexibility in the presentation of data.

The dimensions of the identification feature (normally a portrait) shall be between a minimum of 32.0 mm × 26.0 mm (1.26 in × 1.02 in) and a maximum of 40.0 mm × 32.0 mm (1.57 in × 1.26 in). An issuing State may elect to issue an MRV in this format without an identification feature, replacing it with a crest or symbol.

Though the portrait position is defined as a rectangular area, it may have irregular edges or, if the portrait is digitally printed, have the background dropped out. Such techniques may be used to provide protection against fraudulent alteration.

Affixed photographs (even if protected by a laminate) shall not be applied. Identification features shall be personalized.

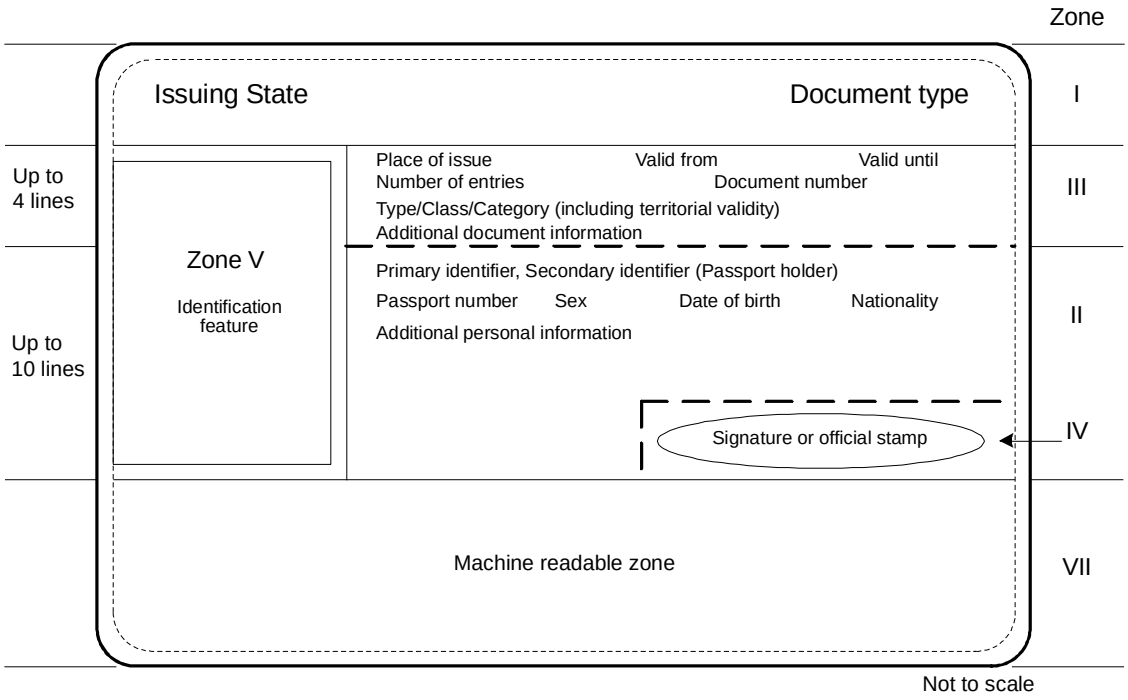


Figure 5. Data elements on a Format A Machine Readable Visa (MRV-A)

Note 1.— Broken lines indicate zone borders whose position may be adjusted by the issuing State to optimize the presentation of the data. Solid lines indicate fixed zone borders. Zone border lines are not printed on the documents.

Note 2.— Provided it is contained within the rectangular area, the identification feature may have irregular edges.

Note 3.— An issuing State may elect to issue a visa with the identification feature replaced by a crest or symbol.

5. TECHNICAL SPECIFICATIONS FOR FORMAT-B MACHINE READABLE VISAS (MRV-B)

This section defines the specifications which are unique to Format-B machine readable visas (MRV-B) and are necessary for global interoperability. Specifications are included for the discretionary expansion of the machine readable data capacity of the MRV beyond that defined for global interchange. The Format-B visa (MRV-B) is suitable for use by States who wish to maintain a clear area on the passport visa page adjacent to the visa, so as to allow a seal to be placed on the visa and the passport page on which it is affixed.

5.1 Dimensions and Placement of the MRV-B

The dimensions and placement of the MRV-B shall be as follows:

MRV-B nominal dimensions. The nominal dimensions of the MRV-B are based on ISO/IEC 7810, ID-2 Type Card as follows:

74.0 mm × 105.0 mm (2.91 in × 4.13 in)

MRV-B margins. The dimensional specifications refer to the outer limits of the MRV-B. A margin of 2.0 mm (0.08 in) along each outer edge, with the exception of the header zone, must be left clear of data.

MRV-B edge tolerances. The edges of the MRV-B shall be within the area circumscribed by the concentric rectangles as illustrated in Figure 6.

Inner rectangle: 73.0 mm × 104.0 mm (2.87 in × 4.09 in)
Outer rectangle: 75.0 mm × 106.0 mm (2.95 in × 4.17 in)

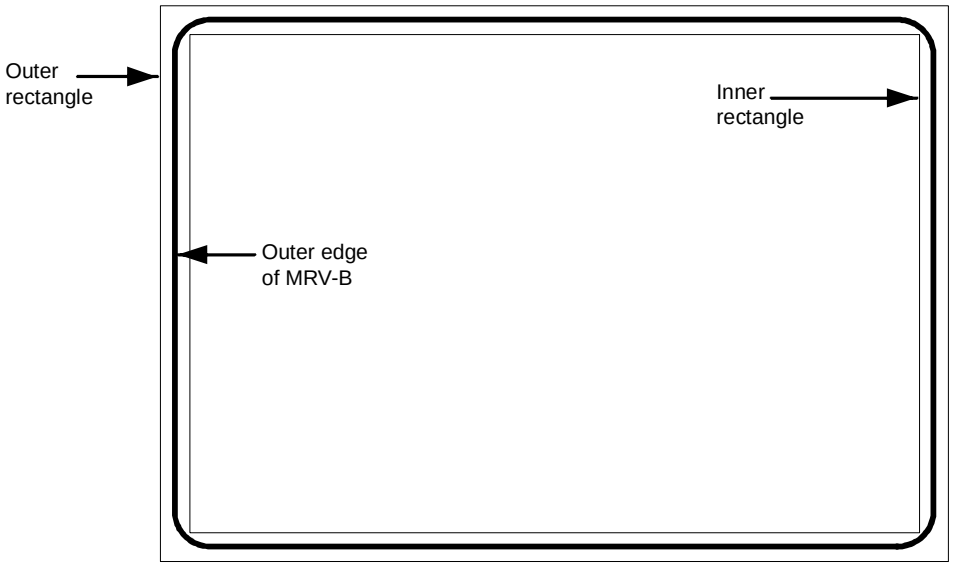


Figure 6. MRV-B dimensional illustration

MRV-B thickness. If the visa is issued as a label, the increase in thickness once the label is attached to the passport visa page shall not exceed 0.19 mm (0.0075 in). The thickness of the area within the machine readable zone (MRZ) shall not vary by more than 0.05 mm (0.002 in). If a protective laminate is used, it is recommended that its thickness not exceed 0.15 mm (0.006 in).

General note.— The decimal notation used in these specifications conforms to ICAO practice. This differs from ISO practice where a decimal point (.) in imperial measurements and a comma (,) in metric measurements is used.

Placement of the MRV-B. The MRV-B shall be positioned as follows:

The MRV-B shall be located on the passport visa page such that the MRZ is coincident with and parallel to the outside edge (*reference edge*) of the passport visa page, and the left edge of the MRV-B is coincident with and parallel to the left edge of the passport visa page as defined in Appendix C, Section C.2.

The MRZ shall be located such that the two OCR lines contained therein are within the Effective Reading Zone (ERZ) as defined in Doc 9303-3.

Only one MRV-B shall be located on a passport visa page (see Appendix C, Section C.2).

6. GENERAL LAYOUT OF THE MRV-B

The MRV-B follows a standardized layout to facilitate reading of data globally, by visual and machine readable means, to accommodate the various requirements of States' laws and practices and to achieve the maximum standardization within those divergent requirements.

The standard layout incorporates space for a portrait of the holder and other identification feature(s). The inclusion of a portrait on a visa is strongly recommended in the interests of security, but States that are not yet able to apply portraits may fill this space with, for example, a national crest.

6.1 MRV-B Zones

An MRV-B is divided into six zones as follows:

Zone I	Mandatory header
Zone II	Mandatory and optional personal data elements
Zone III	Mandatory and optional document data elements
Zone IV	Signature (original or reproduction) or authentication
Zone V	Mandatory zone for identification feature (feature optional)
Zone VII	Mandatory machine readable zone (MRZ)

Note 1.— The signature in Zone IV of a visa is that of an issuing officer, not of the document holder. The signature may be replaced or accompanied by an official stamp.

Note 2.— To facilitate inspection of visas at border control, the layout of the visa presents Zone III above Zone II.

Note 3.— Zone VI is not available on an MRV issued in the form of a label.

Note 4.— Zones I to V constitute the Visual Inspection Zone (VIZ).

Zones I and VII are mandatory. Certain data in Zones II and III are also mandatory. The mandatory components of these four Zones represent the minimum data requirements for an MRV-B. The optional data elements in Zones II, III and V and in optional Zone IV may be utilized to accommodate the diverse requirements of States, while achieving the desired level of standardization. The data elements which may be included in the various zones and their order are set out in Section 7.40. Section 7.4 also illustrates the dimensional specifications and tolerances for the two layouts of the MRV-B and the technical specifications for the printing of data elements within the zones, as well as the guidelines for positioning and adjusting the dimensional specifications of Zones I to V to accommodate the flexibility desired by issuing States. Examples of personalized MRV-Bs are shown in Appendix A, Section A.2. Appendix B, Section B.2 illustrates the format for the presentation of the machine readable data in Zone VII.

6.2 Content, Use and Dimensional Flexibility of Zones

The data elements to be included in the zones, the treatment of the zones and guidelines for the dimensional layout of zones shall be as described hereunder.

Zone I identifies the issuing State and the type of document. These elements are mandatory. The order of the data elements in this zone is left to the discretion of the issuing State.

To facilitate the checking of visas by airline personnel and control authorities, the essential details of the visa document shall be entered in a standard sequence in Zone III while essential personal details of the holder shall be entered in a standard sequence in Zone II. On a visa, Zone III appears above Zone II.

Zone IV provides space for an optional signature or authentication. This is normally the signature of the issuing officer or an official stamp. The application of an official stamp elsewhere on the document is not precluded except that it must not intrude into the MRZ or affect the legibility of entered data.

Zone VII conforms in height to the MRZ defined for all MRTDs so that the machine readable data lines fall within the ERZ specified in Doc 9303-3, thus allowing a single reader to be used for all types and sizes of MRTDs.

All MRZ data elements are mandatory and shall be shown as defined in 0Section 7.2 even though an issuing State may choose not to include a specific MRZ data element in the VIZ.

6.3 Dimensional Flexibility of Zones I to V

Zones I to V may be adjusted in size and shape within the overall dimensional specifications of the MRV-B to accommodate the diverse requirements of issuing States. All zones, however, shall be bounded by straight lines, and all angles where straight lines join shall be right angles (i.e. 90 degrees). It is recommended that the zone boundaries not be printed on the MRV-B. The nominal position of the zones is shown in Section 7.4, Figure 9.

When an issuing State chooses to produce an MRV-B as a securely attached card containing a transparent or otherwise unprintable border around the card, the available area within the zones will be reduced. The full MRV-B dimensions and zone boundaries shall be measured from the outside edge of this border, which is the external edge of the MRV-B.

Zone I shall be adjacent and parallel to the top edge of the MRV-B and extend across the full 105.0 mm ± 1.0 mm (4.13 in ± 0.04 in) dimension. The issuing State may vary the *vertical* dimension of Zone I, as required, but the dimension shall be sufficient to allow legibility of the data elements, and the height shall not be greater than 12.0 mm (0.47 in) as defined in Section 7.4, Figure 9.

Zone V shall be located such that its left edge is coincident with the left edge of the MRV-B, as defined in Section 7.4, Figure 9. Zone V may vary in size but any variation from the nominal dimensions shall not exceed the tolerances specified in Section 7.4, Figure 9.

Zone V may move *vertically* along the left edge of the MRV-B and overlay a portion of Zone I as long as individual details contained in either zone are not obscured. Zone V may, as a result, have its *lower external boundary* coincident with the top edge of the MRZ of the MRV-B and its *upper external boundary* coincident with the top edge of the MRV-B.

The upper boundary of Zone III shall be coincident with the lower boundary of Zone I.

Zone III may extend to the full width of that portion of the MRV-B to the right of Zone V.

The lower boundary of Zone III (see Section 7.4, Figure 9) may be positioned at the discretion of the issuing State. Enough space shall be left for Zone II and Zone IV (when used) below the boundary. The boundary does not need to be straight across the 105.0 mm ± 1.0 mm (4.13 in ± 0.04 in) dimension of the MRV-B.

Normally, the upper boundary of Zone II should be coincident with the lower boundary of Zone III. The boundary does not have to be straight across the 105.0 mm ± 1.0 mm (4.13 in ± 0.04 in) dimension of the visa. Zone II may also overlay a portion of Zone V for the MRV-B if required. When this occurs, issuing States shall ensure that data contained in either zone are not obscured. See Appendix A, A-2.

Zone IV, when included on the MRV-B, shall be entered on the right hand side of the visa immediately above but not intruding into the MRZ. See Section 7.4, Figure 9.

7. DETAILED LAYOUT OF MRV-B

7.1 Visual inspection zone (VIZ) (Zones I-V)

All data in the VIZ shall be clearly legible.

Print spacing. The design of the MRV-B in Zones II and III is based on a vertical line spacing of a maximum of 8 lines per 25.4 mm (1.0 in) and a horizontal printing density of a maximum of 15 characters per 25.4 mm (1.0 in). This spacing has been chosen as the smallest in which information is clear and legible. If any optional field or data element is not used, the entered data may be spread out in the VIZ of the MRV-B consistent with the requirement for sequencing zones and data elements. This horizontal printing density and the font and the vertical line spacing may be adjusted at the discretion of each State, provided that in the VIZ all data shall be printed in a size such that they can be easily read and assimilated by a person with normal eyesight. Typical configurations are shown in Appendix A, A-2. Zone VII, the mandatory MRZ, shall be printed with a line spacing as defined in Section 7.4, Figure 8, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

7.1.1 Data element directory

7.1.1.1 Visual inspection zone — Data element directory

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
01/I Mandatory	Issuing State	The State responsible for issuing the MRV-B. This shall be personalized, the type font being selected at the discretion of the issuing State. For transliteration rules, refer to Doc 9303-3.	Variable	Notes a, c, d, e, i.
02/I Mandatory	Document	The word or words in the language of the issuing State for the document (visa or other appropriate document) which confers on the holder that State's authority to travel to a port of entry in its territory.	Variable	Notes a, c, d, e, i.
03/III Mandatory	Place of issue	Post/location (usually a city) where the MRV-B is issued. A translation of the name into one or more languages, one of which should be English, French or Spanish, shall be given when the translated name is more familiar to the international community.	15	Notes a, b, c, i, k.
04/III Mandatory	Valid from (date)	In most cases this will be the date of issue of the MRV-B and indicates the first date from which the MRV-B can be used to seek entry. For some States the date of issue and the date the visa becomes valid may differ. In such cases the latter shall be indicated in this field and the date of issue may be shown in Field 09 (see below). Date formats are specified in 9303-3.	8	Notes a, b, c, i, k.
05/III Mandatory	Valid until (date)	In most cases this will be the date of expiry of the MRV-B and indicates the last day on which the visa can be used to seek entry. For some States this will be the date by or on which the holder should have left the country concerned. Date formats are specified in 9303-3.	8	Notes a, b, c, i, k.
06/III Mandatory	Number of entries	The number of entries for which the visa is valid.	8	Notes a, b, c, i, k.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
07/III Mandatory	Document number	The number given to the visa by the issuing State.	13	Notes a, b, c, i, j, k.
08/III Mandatory	Type/class/ category	This field shall include one or more of the following elements: • the issuing State's indication of the type and/or class of visa granted in accordance with the law/practice of that State; • the broad categorization of the type of visa granted, e.g. visitor/resident/ temporary resident/student/diplomat, etc., in accordance with the law/practice of the issuing State; • any limitations on the territorial validity of the visa.	46	Notes a, b, c, i, k.
09/III Optional	Additional information	This field may include necessary endorsements as to entitlements which attach to the visa. The issuing State may also use this field to include a) the maximum authorized duration of stay; b) conditions related to the granting of the visa; c) date of issue if different from "Valid from" date; and d) record of any fees paid.		Note g.
10,11/II Mandatory	Name	See Doc 9303-3.	Variable	Notes a, c, i, k.
10/II Mandatory	Primary identifier	See Doc 9303-3.	Variable	Notes a, c, i, k.
11/II Optional	Secondary identifier	See Doc 9303-3.	Variable	Notes a, c, i.
12/II Optional	Passport number	The number of the passport or other travel document in which the MRV-B is placed.	Variable	Notes a, b, c, g, i, j.

Field/ zone no.	*Data element*	*Specifications*	*Maximum no. of character positions*	*References and notes**
13/II Optional	Sex	Sex of MRV-B holder, when included, is to be specified by use of the single initial commonly used in the language of the State of issue. If translation into English, French or Spanish is necessary, followed by an oblique and the capital letter F for female, M for male, or X for unspecified.	3 Fixed	Notes a, f, g.
14/II Optional	Date of birth	See Doc 9303-3.	9	Notes a, b, c, k.
15/II Optional	Nationality	See Doc 9303-3.	Variable	Notes a, h, k.
16/IV Optional	Signature or other authorization	An authorization which may be the signature of an issuing official or an official stamp.		
17/V Mandatory	Identification feature	This field shall appear on the document and should contain a portrait of the holder. If included, the portrait shall have a nominal size of 35.5 ± 3.5 mm (1.40 ± 0.14 in) × 28.5 ± 2.5 mm (1.12 ± 0.1 in). If a State does not place an identification feature in this field, a national symbol or logo may be inserted instead. See Doc 9303-3, Section 3.9 for additional specifications for the portrait.		Note e.

* Notes can be found in 7.2.20.

7.2 Machine Readable Zone (MRZ) (Mandatory Zone VII)

7.2.1 MRZ position, data elements, print specifications and print position in the MRZ

7.2.1.1 MRZ position

The MRZ is located at the bottom of the MRV-B. Section 7.4, Figure 8, shows the nominal position of the data in the MRZ.

7.2.1.2 Data elements

The data elements corresponding to Fields 01, 05, 10, 11, and 13 to 15 of the VIZ are mandatory in the MRZ and shall be printed in machine readable form in the MRZ, beginning with the leftmost character position in each field in the sequence indicated in the data structure specifications shown below. Appendix B, Section B.2, indicates the structure of the MRZ.

7.2.1.3 Print specifications

Machine readable data shall be printed in OCR-B type font, size 1, constant stroke width, as specified in Doc 9303-3. The MRZ shall be printed with the line spacing as defined in Section 7.4, Figure 8, and a horizontal printing density of 10 characters per 25.4 mm (1.0 in).

7.2.1.4 Print position

The position of the left-hand edge of the first character shall be 4.0 mm ± 1.0 mm (0.16 in ± 0.04 in) from the left-hand edge of the document. Reference centre lines for the two OCR lines and a nominal starting position for the first character of each line are shown in Section 7.4, Figure 8. The positioning of the characters is indicated by those reference lines and by the printing zones of the two code lines in Section 7.4, Figure 8 .

7.2.2 Data Structure of Machine Readable Data for the MRV-B

7.2.2.1 Data structure of the upper machine readable line

MRZ field character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 2		Type of document	Capital letter V to designate an MRV. One additional character may be used, at the discretion of the issuing State, to designate a particular type of visa. If the second character position is not used for this purpose, it shall be filled by the filler character (<).	2	Notes a, b, c, e.
3 to 5	1	Issuing State	See Doc 9303-3.	3	Notes a, c, e.
6 to 36	10, 11	Name	See Doc 9303-3.	31	Notes a, c, e.
		Punctuation in the name	Representation of punctuation is not permitted in the MRZ.		Doc 9303-3.

MRZ field character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
		Apostrophes in the name	Components of the name in the VIZ, separated by apostrophes shall be combined, and no filler character (<) shall be inserted. *Example:* VIZ: D'ARTAGNAN MRZ: DARTAGNAN		Doc 9303-3.
		Hyphens in the name	Hyphens (-) in the name shall be converted to the filler character (<) (i.e. hyphenated names shall be represented as separate components). *Example:* VIZ: MARIE-ELISE MRZ: MARIE<ELISE		Doc 9303-3.
		Commas	When a comma is used in the VIZ to separate the primary and secondary identifiers, the comma shall be omitted in the MRZ and the primary and secondary identifiers shall be separated by two filler characters (<<). When a comma is used in the VIZ to separate two name components, it shall be represented in the MRZ by a single filler character (<).		Doc 9303-3.
		Name suffixes	Name suffixes (e.g. Jr., Sr., II or III) shall not be included in the MRZ except as permitted by Doc 9303-3 as components of the secondary identifier.		Doc 9303-3.
		Filler	When all components of the primary and secondary identifiers and required separators (filler characters) do not exceed 31 characters in total, all name components shall be included in the MRZ and all unused character positions shall be completed with filler characters (<) repeated up to		

MRZ field character positions (line 1)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
			position 36 as required.		
		Truncation of the name	When the primary and secondary identifiers and required separators (filler characters) exceed the number of character positions available for names (i.e. 31), they shall be truncated as follows: Characters shall be removed from one or more components of the primary identifier until three character positions are freed, and two filler characters (<<) and the first character of the first component of the secondary identifier can be inserted. The last character (position 36) shall be an alphabetic character (A through Z). This indicates that truncation may have occurred. Further truncation of the primary identifier may be carried out to allow characters of the secondary identifier to be included, provided that the name field shall end with an alphabetic character (position 36). This indicates that truncation may have occurred. When the name consists of only a primary identifier which exceeds the number of character positions available for the name, i.e. 31, characters shall be removed from one or more components of the name until the last character in the name field is an alphabetic character.		Doc 9303-3, Notes a, c, e.

7.2.2.2 Data structure of the lower machine readable line

MRZ field character positions (line 2)	*Field no. in VIZ*	*Data element*	*Specifications*	*Number of characters*	*References and notes**
1 to 9	07 or 12	Passport or document number	At the discretion of the issuing State, either the passport number or the visa number shall be used in this field; however, the latter option can only be exercised where the visa number has 9 characters or fewer. Any special characters or spaces in the number shall be replaced by the filler character (<). The number shall be followed by the filler character (<) repeated up to position 9 as required.	9	Notes a, b, c, e, j.
10		Check digit	See Doc 9303-3.	1	Notes b, e.
11 to 13	15	Nationality	See Doc 9303-3.	3	Notes a, c, e, h.
14 to 19	14	Date of birth	See Doc 9303-3.	6	10.2; Notes b, c, e.
20		Check digit	See Doc 9303-3.	1	Note b.
21	13	Sex	F = Female; M = Male; < = non-specified.	1	Notes a, c, f, g.
22 to 27	5	Valid until (date)	In most cases this will be the date of expiry of the MRV-B and indicates the last day on which the visa can be used to seek entry. For some States this will be the date by or on which the holder should have left. Date formats are specified in 9303-3.	6	Notes b, e.
28		Check digit	See Doc 9303-3.	1	Note b.
29 to 36		Optional data elements	For optional use of the issuing State. Unused character positions shall be completed with the filler character (<) repeated up to position 36 as required.	8	Notes a, b, c, e.

* Notes:

a) Alphabetic characters (A–Z). National characters may be used in the VIZ. In the MRZ, only those characters specified in Doc 9303-3 shall be used.

b) Numeric characters (0–9). National numerals may be used in the VIZ. In the MRZ, only those characters specified in Doc 9303-3 shall be used.

c) Punctuation or other special characters may be used in the VIZ. In the MRZ, only the filler character specified in Doc 9303-3 shall be used.

d) The lengths of fields 01 and 02 are undefined, depending on type font and limits set by MRV-B size and position of other fields.

e) The field caption is not printed on the document.

f) Where an issuing State or organization does not want to identify the sex, the filler character (<) shall be used in this field in the MRZ and an X in this field in the VIZ.

g) The use of a caption to identify a field is at the option of the issuing State.

h) United Nations Laissez-passer are issued to officials of the United Nations Organization under the terms of the *Convention on the Privileges and Immunities of the United Nations* of 13 February 1946 and to officials of the Specialized Agencies of the United Nations under the terms of the *Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations* of 21 November 1947. In the case of visas entered in the United Nations Laissez-passer, in keeping with the international character of United Nations officials, nationality shall not be shown. Instead the appropriate code shall be entered in accordance Doc 9303-3.

i) The number of characters (in the field length) includes any blank spaces.

j) The number of characters in the VIZ may be variable; however, if the document number has more than 9 characters, the 9 principal characters shall be shown in the MRZ in character positions 1 to 9.

k) The field caption shall be printed on the document.

7.2.3 Examples of Names of the Holder in the MRZ

Note.— In the following examples, the document is assumed to be a visa issued by the State of Utopia. The first five characters of the upper machine readable line are coded "V<UTO".

a) Usual representation:

Name: Anna Maria Eriksson
VIZ: ERIKSSON, ANNA MARIA
MRZ (upper line): `V<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<`

b) Central primary identifier:

Name: Deborah Heng Ming Lo
VIZ: HENG, DEBORAH MING LO
MRZ (upper line): `V<UTOHENG<<DEBORAH<MING<LO<<<<<<<<<<`

c) Hyphen as part of the name:

Name: Susie Margaret Smith-Jones
VIZ: SMITH-JONES, SUSIE MARGARET
MRZ (upper line): V<UTOSMITH<JONES<<SUSIE<MARGARET<<<<

d) Apostrophe as part of the name:

Name: Enya Siobhan O'Connor
VIZ: O'CONNOR, ENYA SIOBHAN
MRZ (upper line): V<UTOOCONNOR<<ENYA<SIOBHAN<<<<<<<<<<

e) Multiple name components:

Name: Martin Van Der Muellen
VIZ: VAN DER MUELLEN, MARTIN
MRZ (upper line): V<UTOVAN<DER<MUELLEN<<MARTIN<<<<<<<<

f) No secondary identifier:

Name: Arkfreith
VIZ: ARKFREITH
MRZ (upper line): V<UTOARKFREITH<<<<<<<<<<<<<<<<<<<<<<

7.2.3.1 Truncated names — Secondary identifier truncated

a) One or more name components truncated to initials:

Name: Nilavadhanananda Chayapa Dejthamrong Krasuang
VIZ: NILAVADHANANANDA, CHAYAPA DEJTHAMRONG KRASUANG
MRZ (upper line): V<UTONILAVADHANANANDA<<CHAYAPA<DEJ<K

b) One or more name components truncated:

Name: Nilavadhanananda Arnpol Petch Charonguang
VIZ: NILAVADHANANANDA, ARNPOL PETCH CHARONGUANG
MRZ (upper line): V<UTONILAVADHANANANDA<<ARNP<PE<CHARO

7.2.3.2 Truncated names — Primary identifier truncated

a) One or more components truncated to initials:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): V<UTOBENNELONG<WOOLOOMOOLOO<WAR<W<<D

b) One or more components truncated:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): V<UTOBENNELONG<WOOLOOM<WAR<WA<<DINGO

c) One or more components truncated to a fixed number of characters:

Name: Dingo Potoroo Bennelong Wooloomooloo Warrandyte Warnambool
VIZ: BENNELONG WOOLOOMOOLOO WARRANDYTE WARNAMBOOL, DINGO POTOROO
MRZ (upper line): V<UTOBENN<WOOL<WARR<WARN<<DINGO<POTO

7.2.3.3 Names that just fit, indicating possible truncation by letter in the last position of the name field, but which are not truncated

Name: Stephen Trevor Papandropoulous
VIZ: PAPANDROPOULOUS, STEPHEN TREVOR
MRZ (upper line): V<UTOPAPANDROPOULOUS<<STEPHEN<TREVOR

Note.— Even though there is an alphabetic character in the 36th character position of this MRV-B upper machine readable line, this name has not been truncated but it shall be assumed that it has been truncated.

7.3 Portrait

Portrait. For the MRV Format-B the rectangular area defined in the data element directory as Zone V should contain a portrait. Such portrait, if included, shall represent only the holder of the MRV-B.

Portrait edges. The portrait may have irregular edges. When a digitally printed reproduction is used, the background of the portrait may be dropped out in order to provide protection against forgery or substitution.

Zone V without an identification feature. A standard default image, such as a national symbol, crest or wording, should be selected and used in Zone V when an identification feature is not included.

7.4 MRV-B Diagrams

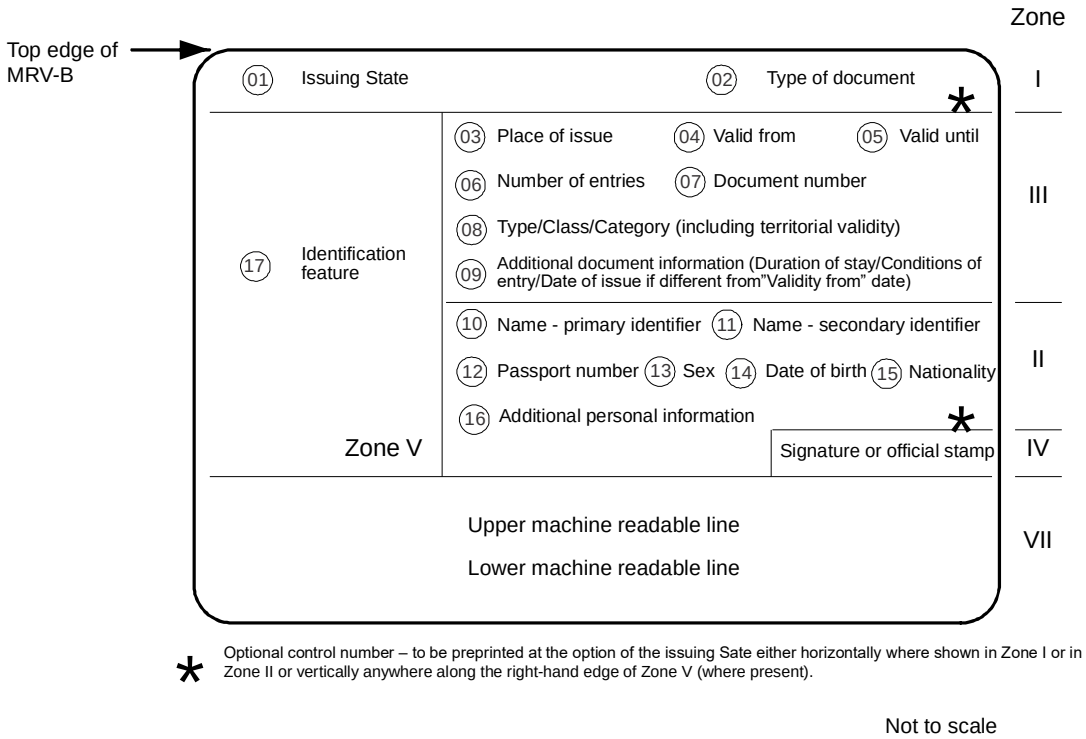


Figure 7. Location of data elements on an MRV-B.

Note 1.— VIZ based on maximum printing density of 8 lines per 25.4 mm (1.0 in) and horizontal printing density of 15 characters per 25.4 mm (1.0 in).

Note 2.— MRZ based on horizontal printing of 10 characters per 25.4 mm (1.0 in).

Note 3.— ◯ = field numbers.

Note 4.— The borderlines of the zones are not printed on the actual visa.

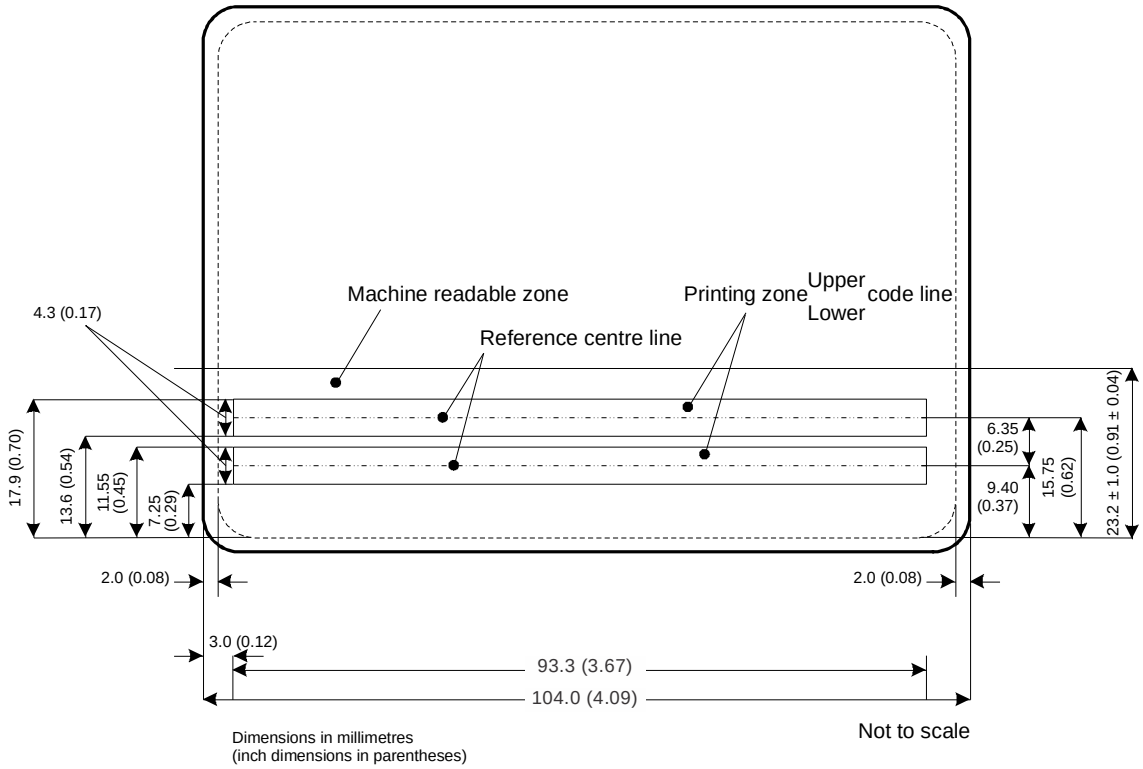


Figure 8. Schematic diagram of the Machine Readable Zone of an MRV-B.

Note.— For illustration purposes, the smallest option for the 105.0 mm (4.13 in) dimension of the MRV-B and the smallest option for the left-hand margin in the MRZ have been selected.

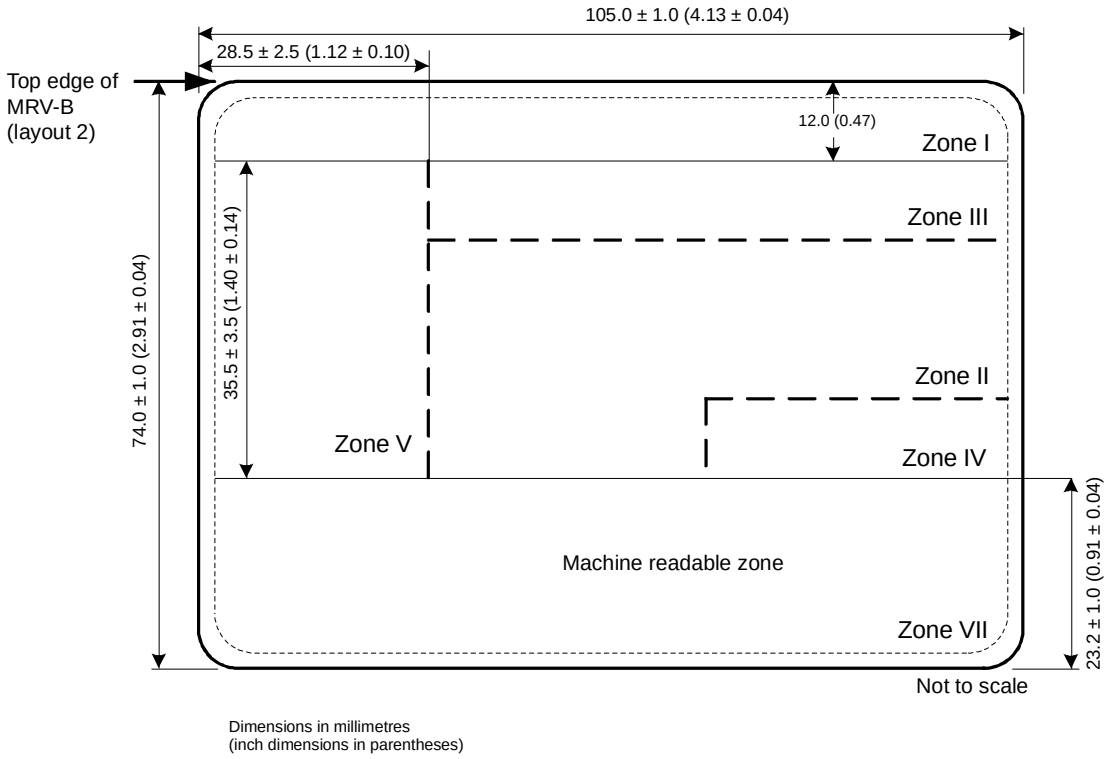


Figure 9. Nominal positioning of zones on an MRV-B.

This diagram should be considered in conjunction with Section 6.2. It assumes that all the available space for data in the Visual Inspection Zone is used. The line spacing in the VIZ is the closest permitted at 8 lines per 25.4 mm (1.0 in). If an issuing State requires less information the line spacing can be increased to print fewer lines in the VIZ.

Dotted lines indicate zone boundaries whose positions are not fixed, enabling issuing States flexibility in the presentation of data.

The dimensions of the identification feature (normally a portrait) shall be between a minimum of 32.0 mm × 26.0 mm (1.26 in × 1.02 in) and a maximum of 39.0 mm × 31.0 mm (1.54 in × 1.22 in). An issuing State may elect to issue an MRV in this format without an identification feature, replacing it with a crest or symbol.

Though the portrait position is defined as a rectangular area, it may have irregular edges or, if the portrait is digitally printed, have the background dropped out. Such technique may be used to provide protection against fraudulent alteration.

Affixed photographs (even if protected by a laminate) shall not be applied. Identification features shall be personalized.

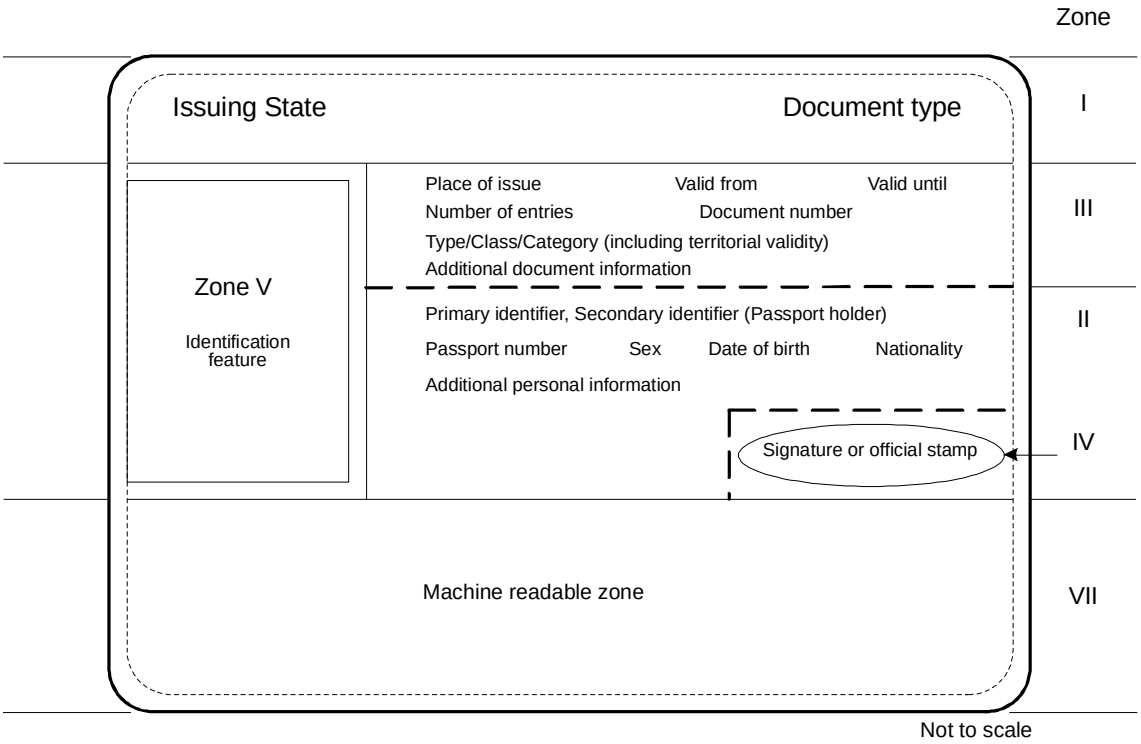


Figure 10. Data elements on a Format B Machine Readable Visa (MRV-B).

Note 1.— Broken lines indicate zone borders whose position may be adjusted by the issuing State to optimize the presentation of the data. Solid lines indicate fixed zone borders. Zone border lines are not printed on the document.

Note 2.— Provided it is contained within the rectangular area, the identification feature may have irregular edges.

Note 3.— An issuing State may elect to issue a visa with the identification feature replaced by a crest or symbol.

8. USE OF OPTIONAL BARCODES ON MACHINE READABLE VISAS

8.1 Scope

This section defines the specifications governing the use of one or more bar codes on an MRV, at the discretion of the issuing State, to allow expansion of the machine readable data capacity.

8.2 Definition

A bar code is defined as a linear or two-dimensional bar code conforming with the specifications defined herein and capable of representing data therein and encoded data read therefrom.

8.3 Location of Bar Code(s)

Figures 11 and 12 illustrate the location of a bar code on the MRV-A and MRV-B, respectively, as well as the specifications for the exact placement and overall dimensions of the area to house any optional bar codes. It should be noted that the height and width of the bar code(s) area can vary up to the maximum dimensions shown. In defining these dimensions, the trade-off between optional expanded machine readable data capacity desired and accommodation of mandatory and optional details (VIZ) should be considered.

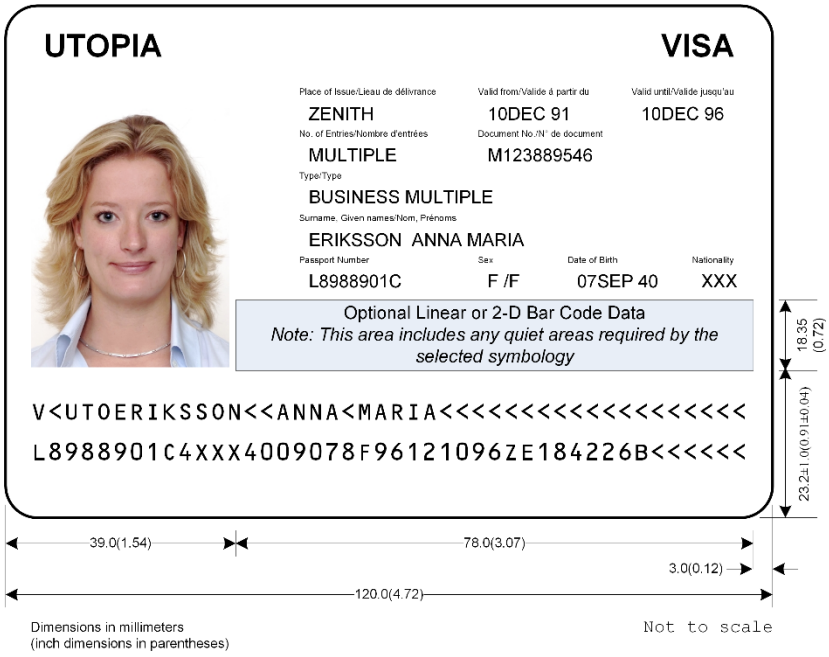


Figure 11. Format-A machine readable visa with optional linear or two dimensional bar code

Figure 12. Format-B machine readable visa with optional linear or two dimensional bar code

8.4 Quality of Bar Code(s)

The bar code(s) included in the bar code(s) area shall meet the overall symbol grade defined for the chosen symbology (symbologies) that allows symbols to be read, following final assembly of the MRV, most times in a single pass.

8.5 Symbologies and Logical Data Structure

In order to have the capability to support global data interchange with authorized bodies such as airlines, the bar code symbology selected must offer sufficient data storage capacity to accommodate all mandatory data elements included in the mandatory data groups and in any optional data groups which may be selected from the logical data structure as developed for optional capacity expansion technologies. Furthermore, the associated reading software must be available in the public domain.

8.6 Machine Reading of the Bar Code(s)

To enable accurate reading of bar code(s) coexisting with security treatments (e.g. background security printing) in the bar code(s) area, and the use of a single machine reader for reading the MRZ and the bar code(s), where desired by a State, the bar code(s) optionally included on the MRV shall be printed such that the bar code(s) absorb(s) in the B900 band as defined in ISO 1831 (i.e. near infra-red). The bar code(s) may be visually legible.

In determining the placement of the bar code on the MRV, issuing States shall accommodate any special needs or operating conditions of the symbology (symbologies) such as bit area and error correction level. In addition, sufficient marginal space shall be included to accommodate “quiet areas”.

Issuing States are encouraged to locate the bar code(s) area nearest to the top edge of the MRZ to allow for possible use of the optical sensing components from the OCR reader, supported by bar code interpretation logic, to accommodate reading of optional bar code data.

The bar code(s) optionally included in the bar code(s) area of the MRV shall not interfere with the accurate reading of data from the MRZ.

9. USE OF OPTIONAL DIGITAL SEALS FOR VISA DOCUMENTS

Doc 9303-13 specifies Visible Digital Seals (VDS) for non-electronic documents. In this section the specific rules and requirements for the use of Visible Digital Seals on Visa documents are described.

9.1 Content and Encoding Rules

9.1.1 Header

The Document Feature Definition Reference for this use-case is 93dec. The Document Type Category for Visas is 0x01. Otherwise, the content of the header is the same as defined in Doc 9303-13, Section 3.1.1.

9.1.2 Document Features of a VDS for Visas

The following document features are stored in the seal:

Machine Readable Zone (REQUIRED)

The Machine Readable Zone (MRZ) of a visa contains the following information:

- issuing state
- primary and secondary identifier
- passport or visa number
- nationality of the document holder
- date of birth of the document holder
- sex of the document holder
- validity period (valid until …)

Some countries may not issue paper based visas, but instead use a domestic database to store visa applications, and merely attach a confirmation sticker to the passport. If such countries choose to adopt this standard for such stickers, the above information SHALL be encoded as either the MRZ of an MRV-A or MRV-B.

Additionally, the following document features are stored:

Number of Entries (OPTIONAL)

The number of times the visa holder may enter the territory for which the visa is valid.

Duration of Stay (REQUIRED)

This feature denotes the number of days, months or years during which the visa holder may stay in the territory for which the visa is valid. Note that this is distinct from the valid-until date of the MRZ, which is already stored in the Visa-MRZ: First, it is remarked that in most cases this [Valid-Until field of the Visa-MRZ] will be the date of expiry of the MRV and indicates the last day on which the visa can be used to seek entry. For some States this will be the date by or on which the holder should have left. Second, for some issuing countries the stay must be continuous, and for others, the stay can spread over several periods. Thus, to avoid ambiguity during validation, the feature for the duration of stay is required.

Passport Number (REQUIRED)

This feature denotes the number of the passport to which the visa sticker is attached. The passport number might already be present in the MRZ: it is remarked that at the discretion of the issuing State, either the passport number or the visa number SHALL be used in this field [document number field of the Visa-MRZ]; however, the latter option can only be exercised where the visa number has 9 characters or fewer. To avoid ambiguity during validation, the field for the passport number (separate from the MRZ) is required.

Visa Type (OPTIONAL)

This feature encodes the type of the visa. The field is especially intended to be used, if the type of the visa is not encoded as the second letter of the MRZ.

Additional Feature Field (OPTIONAL)

Reserved for future use. This field is OPTIONAL, and intended to store additional verification information in future versions of this standard.

9.1.3 Encoding Rules for Document Features

In the following, the digital encoding of document features of the visa seal is defined.

MRZ of Machine-Readable Visa of Type A (MRV-A, see section 4.2.2)

Tag: 0x01
Min. Length: 48 Byte
Max. Length: 48 Byte Value Type: Alphanumeric
Required: Required (if visa is of type MRV-A)
Content: The first line of the MRZ of an MRV-A (44 chars.) and the first 28 chars. of the second line of the MRZ of an MVR-A, concatenated and encoded by C40. The filler symbol < in the MRZ is replaced by <SPACE> prior to encoding by C40.

MRZ of Machine-Readable Visa of Type B (MRV-B, see section 7.2.2)

Tag: 0x02
Min. Length: 44 Byte
Max. Length: 44 Byte Value Type: Alphanumeric
Required: Required (if visa is of type MRV-B)
Content: The first line of the MRZ of an MRV-B (36 chars.) and the first 28 chars. of the
second line of the MRZ of an MVR-B, concatenated and encoded by C40. The filler symbol < in the MRZ is replaced by <SPACE> prior to encoding by C40.

Number of Entries

Tag: 0x03
Min. Length: 1 Byte
Max. Length: 1 Byte Value Type: Integer
Required: Optional
Content: The integer in the range of 0-255dec encodes the number of allowed entries. A value of 0 denotes unlimited entries.

Duration of Stay

Tag: 0x04
Min. Length: 3 Byte

Max. Length: 3 Byte Value Type: Integer
Required: Mandatory
Content: The duration of stay is encoded as specified in Table 1.

Table 1: Encoding for the Duration of Stay

Integer Values of			Meaning
Byte 1	**Byte 2**	**Byte 3**	
0	0	0	The *valid-until* field of the MRZ denotes the last day on which the visa holder may stay in the country for which the visa was issued.
255	255	255	The *valid-until* field of the MRZ denotes the last day on which the visa holder may seek entry at the border for which the visa was issued. The duration of stay is determined by the authorities at the time of entry at the border.
number of days	number of month	number of years	The duration of stay is the sum of the number of days, the number of month, and the number of years, calculated from the time on which the visa holder enters the country for which the visa was issued. The *valid-until* field of the MRZ denotes the last day on which the visa-holder may seek entry. The triples (0,0,0) and (255,255,255), are reserved and, as seen above, MUST NOT be used in this case.

Passport Number

Tag: 0x05
Min. Length: 6 Byte
Max. Length: 6 Byte Value Type: Alphanumeric Required: Mandatory
Content: The passport number of the passport of the applicant on which the visa sticker is attached.

Visa Type

Tag: 0x06
Min. Length: 1 Byte
Max. Length: 4 Byte Value Type: Binary
Required: Optional
Content: The visa type is encoded as a binary sequence.

Additional Feature

Tag: 0x07
Min. Length: 0 Byte
Max. Length: 254 Byte Value Type: Binary
Required: Optional
Content: Reserved for future use by ICAO.

9.2 Visa Signer and Seal Creation

With respect to this Visa profile, Visa Signer Certificates are issued in a way that allows verification by CSCA certificates. A possible architecture and implementation for the Visa signer and its client is described in Doc 9303-13, Section 3.2.1.

For the security of the Visa signing system, see Doc 9303-13, Section 3.2.2

9.3 Public Key Infrastructure (PKI) and Certificate Profiles

In general the requirements from Doc 9303-12, Section 4.3 apply. The following deviations apply due to the specific characteristics and properties of Visa documents.

Visa specific validity periods are as follows:
Private Key Usage Time for Visa signer certificates: 1 to 2 years

9.4 Validation Policy Rules (Informative)

For the validation policy of digital seals on visas, all rules from Doc 9303-13, Appendix D are valid. In addition the following rules to determine the validity of the digital seal apply.

In addition to the generic document Validation Policy the policy for Visas considers the following questions:
1. Is the MRZ of the passport valid?
2. Does the MRZ of the passport match with the MRZ of the visa?

Below we give the additional Visa specific validation rules for each type of control, list the validation criteria, expected results for each criteria, and resulting status sub-indications.

Visible Digital Seal Validation

1. Visa-MRZ Validation
   - if the checksums of the visa MRZ are not compliant with the applicable norm – dependent on the visa type – then the status is INVALID with sub-indication INVALID_VISA_MRZ
   - If there is a mismatch between a field of the Visa MRZ and the corresponding document feature stored within the seal, then the status is INVALID with SEAL_VISA_MISMATCH. Additional information on the mismatch SHOULD be provided. Otherwise, continue.

2. Passport MRZ Validation
   - If the checksums of the passport MRZ are not compliant with the applicable norm – dependent on the passport type – then the status is INVALID with sub-indication INVALID_PASSPORT_MRZ. Otherwise continue.

3. Passport-link Validation
   - If any of the fields of the passport MRZ listed as follows do not correspond to their equivalent feature stored in the digital seal, then the status is INVALID with sub- indication SEAL_PASSPORT_MISMATCH. The MRZ fields of the passport are: 1.) passport number and 2.) passport issuing country. Otherwise if all fields match, the status of the Visible Seal is VALID.

The generic and Visa specific validation rules cover a comparison of the data stored in the seal against data stored on the MRZ of the visa and the passport. On top of that, a manual inspection of those data that are stored in the seal and printed on the visa, but are not present in the MRZ of the visas, could be conducted.

Table 2: Recommended Trust Levels of the Visa Policy for Visa specific sub status indications

Status Indication	Sub Status Indication	Trust Level
INVALID	INVALID_VISA_MRZ	*high fraud potential*
	SEAL_VISA_MISMATCH	

INVALID_PASSPORT_MRZ
SEAL_PASSPORT_MISMATCH

10. REFERENCES (NORMATIVE)

Certain provisions of the following international Standards, referenced in this text, constitute provisions of Part 7 of Doc 9303. Where differences exist between the specifications contained in Part 7 and the referenced Standards, to accommodate specific construction requirements for machine readable travel documents, including machine readable visas, the specifications contained herein shall prevail.

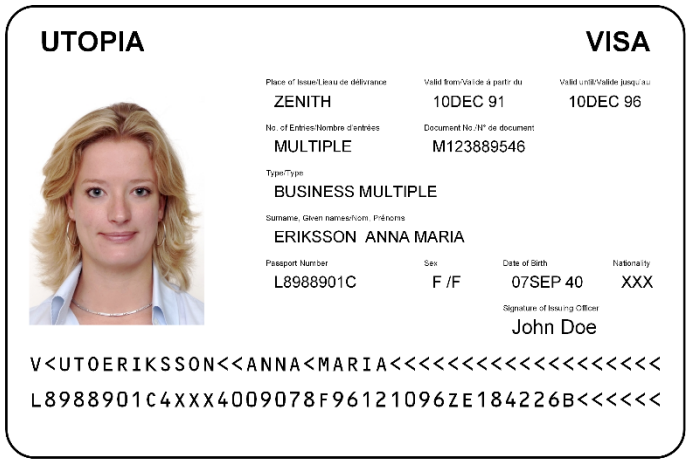
ISO/IEC 7810	ISO/IEC 7810 : 2003, Identification cards — Physical characteristics
ISO 1831	ISO 1831 : 1980, Printing specifications for optical character recognition

— — — — — — — —

Appendix A to Part 7

EXAMPLES OF PERSONALIZED MRVs (INFORMATIVE)

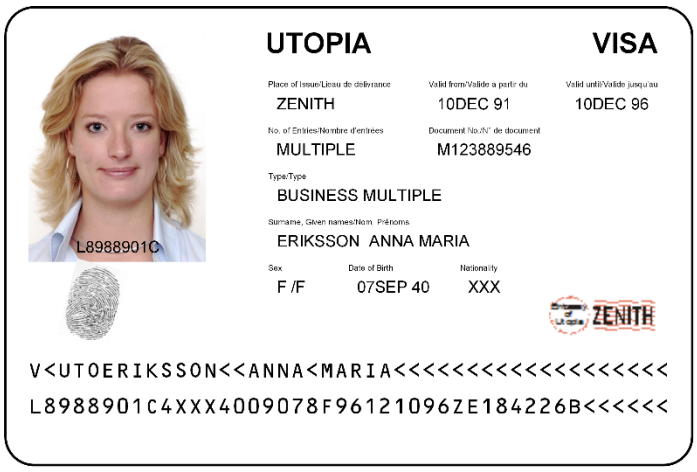
A.1 MRV-A EXAMPLES



Not to scale

Figure 13. Example illustrates an MRV-A with:

- **Zones I, III, II, IV, V and VII;**
- **a holder with unspecified nationality (i.e. "XXX").**



Not to scale

Figure 14. Example illustrates an MRV-A the same as Figure 13 but with:

- **Zone V increased in size to accommodate fingerprint and thus overlaying part of Zone I;**
- **part of Zone II (passport number) overlaying Zone V; and**
- **an issuing office stamp instead of the signature in Zone IV.**

A.2 MRV-B Examples

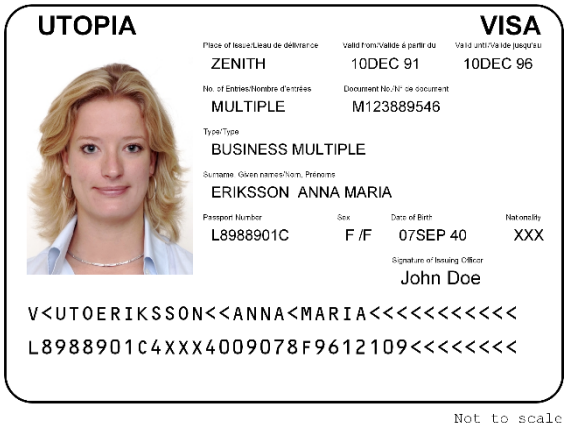


Figure 15. Example illustrates an MRV-B with:

- **Zones I, III, II, IV, V and VII;**
- **a holder with unspecified nationality (i.e. "XXX").**

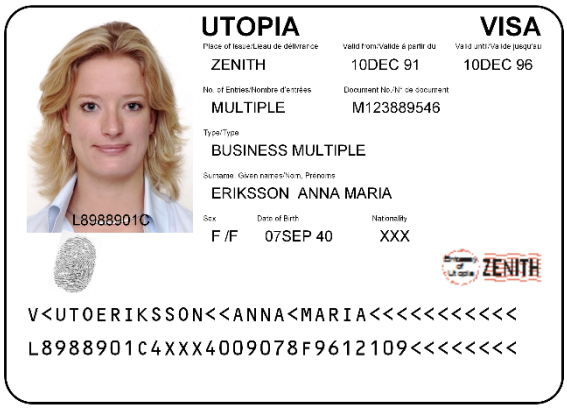


Figure 16. Example illustrates an MRV-B the same as Figure 15 but with:

- **Zone V increased in size to accommodate fingerprint and thus overlaying part of Zone I;**
- **part of Zone II (passport number) overlaying Zone V; and**
- **an issuing office stamp instead of the signature in Zone IV.**

— — — — — — — —

Appendix B to Part 7

CONSTRUCTION OF THE MRZ (INFORMATIVE)

B.1 MRV-A MRZ-CONSTRUCTION

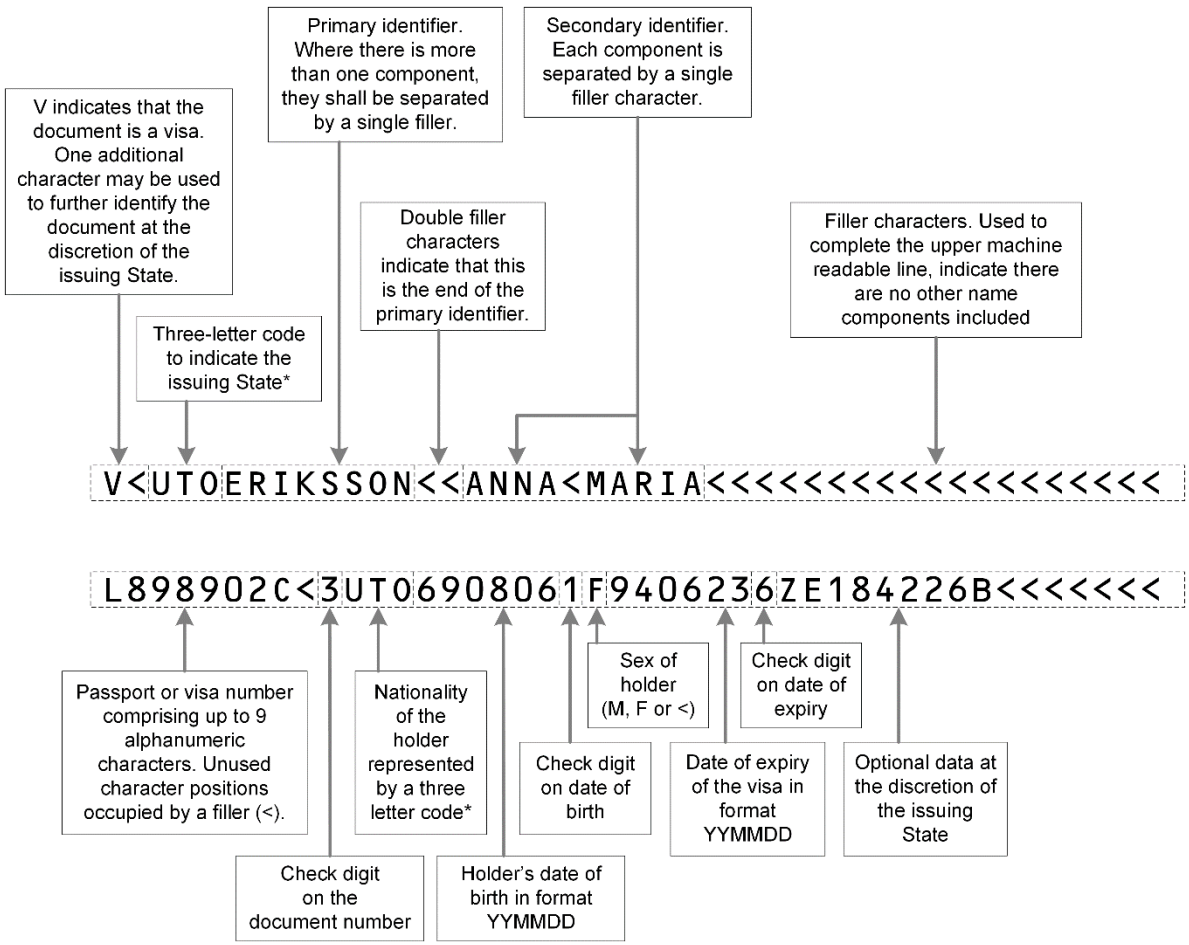


Figure 17. MRV-A MRZ construction:

- ***Three letter codes are given in Doc 9303-3.**
- **Dotted lines indicate data fields; these, together with arrows and comment boxes, are shown for the reader's understanding only and are not printed on the document.**
- **Data are inserted into a field beginning at the first character position starting from the left. Any unused character positions shall be occupied by filler characters (<).**

B.2 MRV-B MRZ-Construction

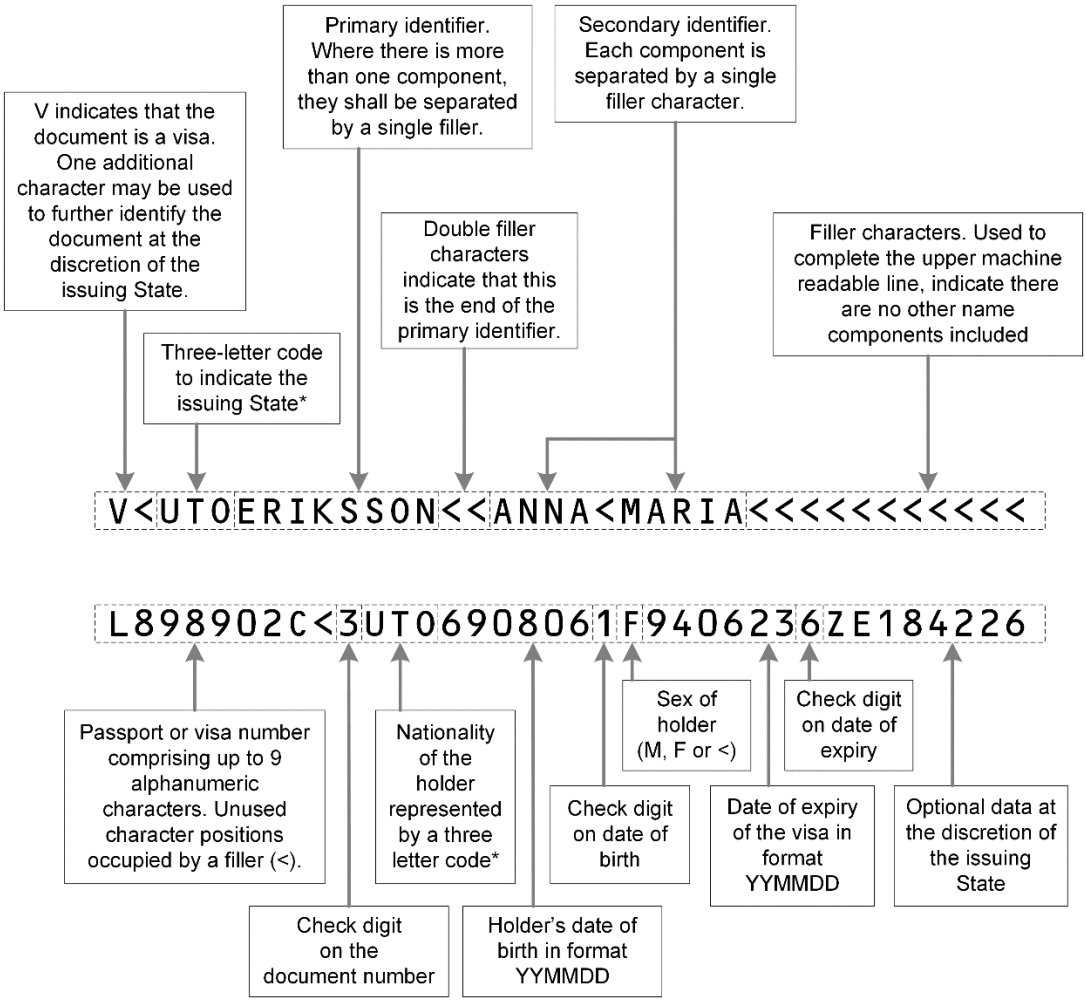


Figure 18. MRV-B MRZ construction:

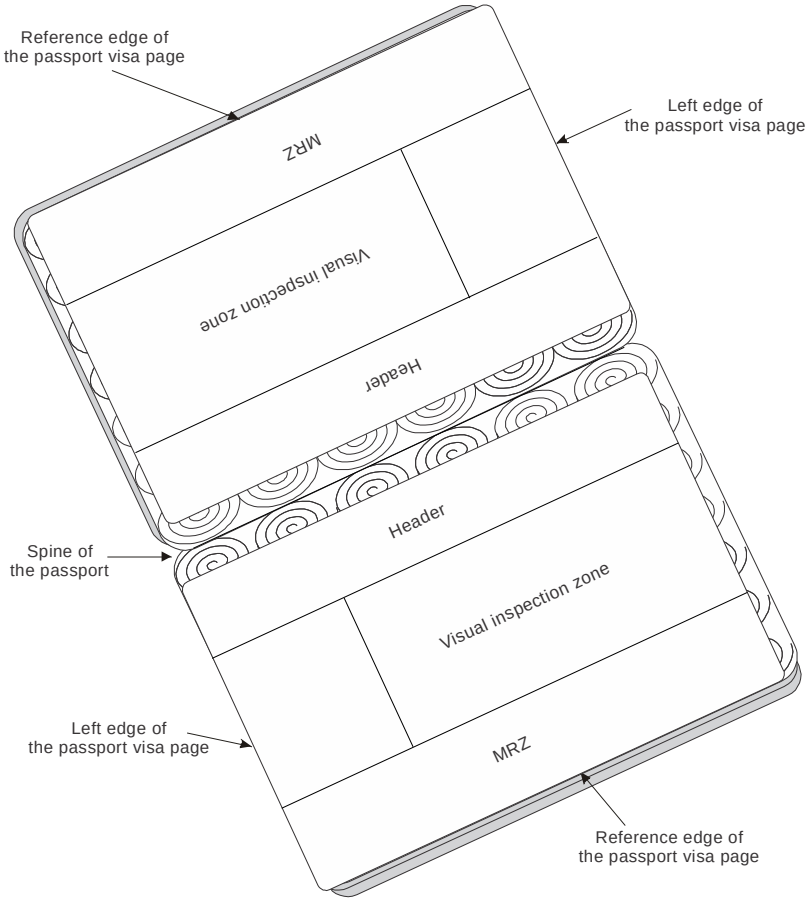
- ***Three letter codes are given in Doc 9303-3.**
- **Dotted lines indicate data fields; these, together with arrows and comment boxes, are shown for the reader's understanding only and are not printed on the document.**
- **Data are inserted into a field beginning at the first character position starting from the left. Any unused character positions shall be occupied by filler characters (<).**

— — — — — — — —

Appendix C to Part 7

POSITIONING IN PASSPORT (INFORMATIVE)

C.1 MRV-A POSITIONING

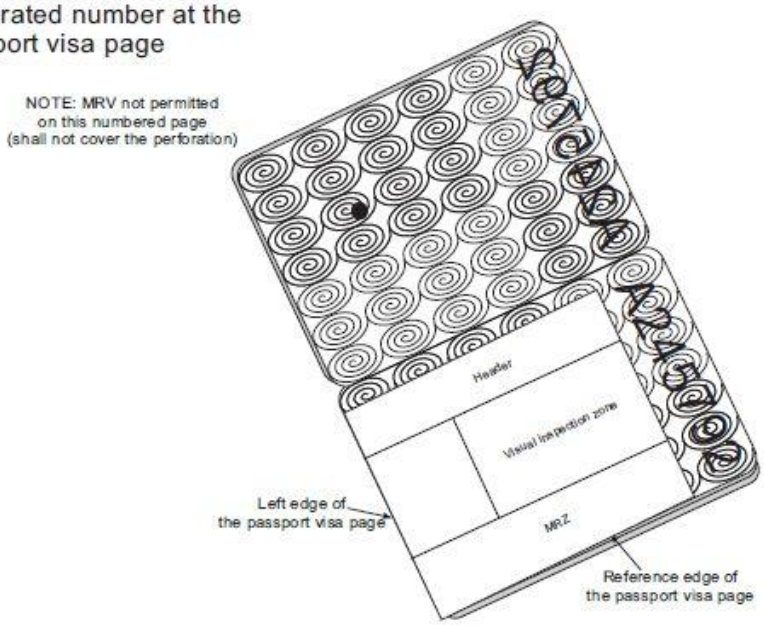


Each MRV shall be placed so that:

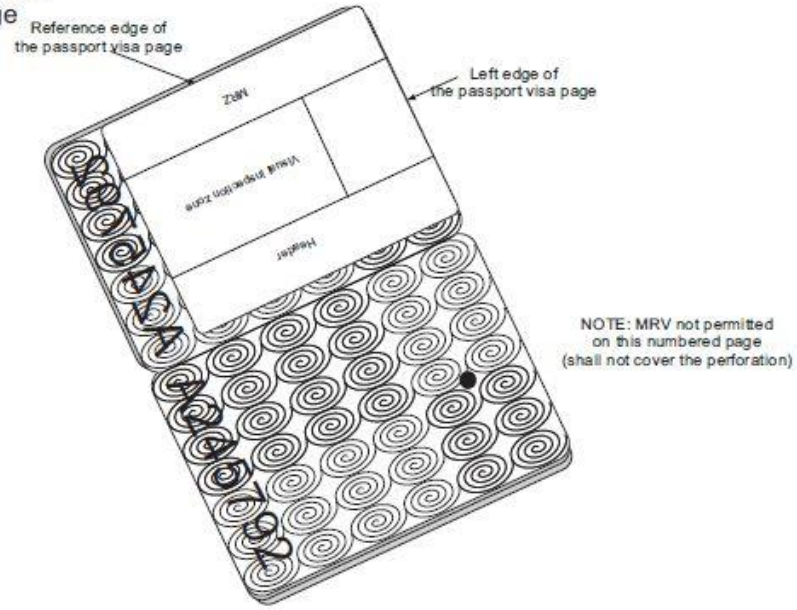
- the two OCR lines of the MRZ are parallel to the appropriate reference edge of the passport visa page;
- the leading characters of each OCR line are positioned with respect to the left edge of the passport visa page;
- the MRZ is immediately adjacent to the appropriate reference edge of the passport visa page;
- and no MRV may be placed on top of another, nor on the reverse of a page that already has an MRV affixed, nor on the reverse of an MRP data page.

C.2 MRV-B POSITIONING

Example 1:
Printed or perforated number at the top of the passport visa page



Example 2:
Printed or perforated number at the bottom of the passport visa page



— — — — — — — —

Appendix D to Part 7

MATERIALS AND PRODUCTION METHODS (INFORMATIVE)

Note 1.— The following information reflects some past as well as current practices of MRV producers and is included here for guidance only. It is not an endorsement of any product or method.

Note 2.— It is the responsibility of the issuing State to ensure that the MRV selected for issue is constructed in such a way that the document will perform satisfactorily for its required life.

Traditionally, visas have taken the form either of a label affixed to a page of the holder's passport or the application of an imprint onto the passport page usually with manual infilling for the personalization. Manual infilling is obviously impractical for machine readable visas where very precise characters for optical recognition are required. There is no fundamental reason why a visa should not be imprinted onto a passport page using a printer capable of printing OCR-B. However, an issuing State that elects to do this will find that many passports, which, of course, are issued by other States, have printed or perforated numbers or other printing on their pages which can absorb the infra-red light used by the document reader and result in a failure to read at border control. In general, therefore, it is better to use a machine readable visa in the form of a label affixed to the passport page.

An MRV can have a life limited to a single entry into a country or it can allow multiple entries over the life of the passport or beyond. The issuing State should ensure that the MRV is appropriately durable for the required life. States should also ensure that their visas are resistant to fraud. States can achieve considerable protection against these threats where border control has access to a central database containing the details of the issuance of genuine visas. However this is not always practicable. The threats are:

- total counterfeiting of the document;
- removal of a visa from one passport and its placement in another;
- alteration of the personal information or validity data.

Substrate. Visas have been produced using either paper or a synthetic polymer as the substrate. The substrate should have adequate opacity to prevent any printing or perforations on the passport page affecting the machine reading. The substrate should exhibit no visible fluorescence when irradiated by ultra violet light. Common choices of security features for paper have included: chemical reactants, iridescent plaquettes, fibres (silk and/or synthetics, visible and/or invisible, fluorescent and/or non-fluorescent), and security threads. Synthetic polymer substrates may also incorporate some of these security features. Care must be taken to ensure that any chemical reactants used are unaffected by the adhesive used to affix the visa. It is desirable that the substrate be damaged by attempts to alter the data on the visa or to remove it from the passport. The damage may take the form of tearing or distortion.

Inks. Inks that are chemically fugitive, fluorescent, heat sensitive, and optically variable are means of enhancing security in the MRV.

Printing. Fine line printing, rainbow (split fountain) printing using guilloche patterns, intaglio printing, and incorporation of concealed images into the design are methods of enhancing both the security and aesthetics of the MRV.

Adhesive. Water-moistenable or pressure-sensitive adhesives have been used to affix visas into passports. The selected adhesive should achieve and maintain a strong bond even when heated. The adhesive/substrate combination should be such that the substrate tears or distorts before the adhesive bond fails.

Die cutting. Though the final size and shape of the visa is defined in these specifications, the size is too small for most types of visa infilling printers. It is therefore normal for an issuing State to procure visas in a sheet form suitable for the infilling printer with one or more visas contained within the sheet area, the visas being die cut to shape. It is important to ensure compatibility between the sheets of visas and the printer to ensure that the visas do not become separated from the carrier sheet in the printer. It is also important to ensure that the edges of the sheet or of the die-cut shape are not contaminated with adhesive which can build up in the printer and result in misfeeding. Consistency of position of the die-cut shape relative to the edges of the sheet is important to ensure that the machine readable information is placed within the ERZ.

Personalization. Most forms of variable image printing, including laser (covered by a laminate), ink jet, dye sublimation and dot matrix printing have been used in the personalization of visas, with the first three used where a portrait is required. To minimize the risk of fraudulent removal of the personalization, the selected combination of substrate and infilling method should achieve a high penetration of the image into the substrate or a strong bond between the material forming the image and the substrate.

Protecting the personalization. Protective laminate or lacquer layers may be used to secure the data on the visa. Any laminate material should be firmly bonded to the substrate so that disruption of the substrate or destruction of the laminate material occurs when attempts are made to remove the laminate.

Appendix E to Part 7

WORKED EXAMPLE VISIBLE DIGITAL SEAL FOR VISA DOCUMENT (INFORMATIVE)

The following example shows a visible digital seal that results from encoding the data shown in Table 4. To generate the signature, ECDSA-256 with the curve brainpoolP256r1 was used. The domain parameters of brainpoolP256r1 and the private key encoded as Base64 are:

```
-----BEGIN EC PARAMETERS-----
MIHgAgEBMCwGByqGSM49AQECIQCp+1fboe6pvD5mCpCdg41ybjv2I9UmICggE0
gd
H25TdzBEBCB9Wgl1/CwwV+72dTBBev/n+4BVwSbcXGzpSktE8zC12QQgJtxcbO
lK
S0TzMLXZu9d8v5WEFilc9+HOa8zcGP+MB7YEQQSL0q65y35XyyxLSC/8gbevud
4n
4eO9I8I6RFO9ms4yYlR++DXD2sT9l/hGGhRhHcnCd0UTLe2OVFwdVMcvBGmXAi
EA qftX26Huqbw+ZgqQnYONcYw5eqO1Yab3kB4OgpdIVqcCAQE=
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MIIBUQIBAQQgNN2C+Njrq+F9bmAQ5FEgW/GCdul78V+XgV9h+dMyw7eggeMwge
AC
AQEwLAYHKoZIzj0BAQIhAKn7V9uh7qm8PmYKkJ2DjXJuO/Yj1SYgKCATSB0fbl
N3
MEQEIH1aCXX8LDBX7vZ1MEF6/+f7gFXBJtxcbOlKS0TzMLXZBCAm3Fxs6UpLRP
Mw
tdm713y/lYQWKVz34c5rzNwY/4wHtgRBBIvSrrnLflfLLEtIL/yBt6+53ifh47
0j
wjpEU72azjJiVH74NcPaxP2X+EYaFGEdycJ3RRMt7Y5UXB1Uxy8EaZcCIQCp+1
fb
oe6pvD5mCpCdg41xjDl6o7VhpveQHg6Cl0hWpwIBAaFEA0IABB1CQwfc2PkvPY
Ku
gQ3qA0tqEhzH0ox4M9cOq8ajzKotHG2jrwlIuHaemRad0qG1pltDHgZOC59HwI
0P yLNvXHc=
-----END EC PRIVATE KEY-----
```

Encoding input data yields a byte stream, which are both depicted in Table 4. Hashing the header (cf. Table 3) and message with SHA-256 and signing them with the above private key gave the following signature (r,s):

```
r:
56BCBFEDFD2DC884247426A240A7068D32B37C6CE370AEEAB62B548B5FCC16FA
s:
6A098CA74CB22559435FD4DBDE709B45F6FC4C850DA421A6E75CD05A88707CBB
```

For the sake of completeness, the signature as DER encoded ASN.1:

```
3044022056bcbfedfd2dc884247426a240a7068d32b37c6ce370aeeab6
2b
548b5fcc16fa02206a098ca74cb22559435fd4dbde709b45f6fc4c850d
a4 21a6e75cd05a88707cbb
```

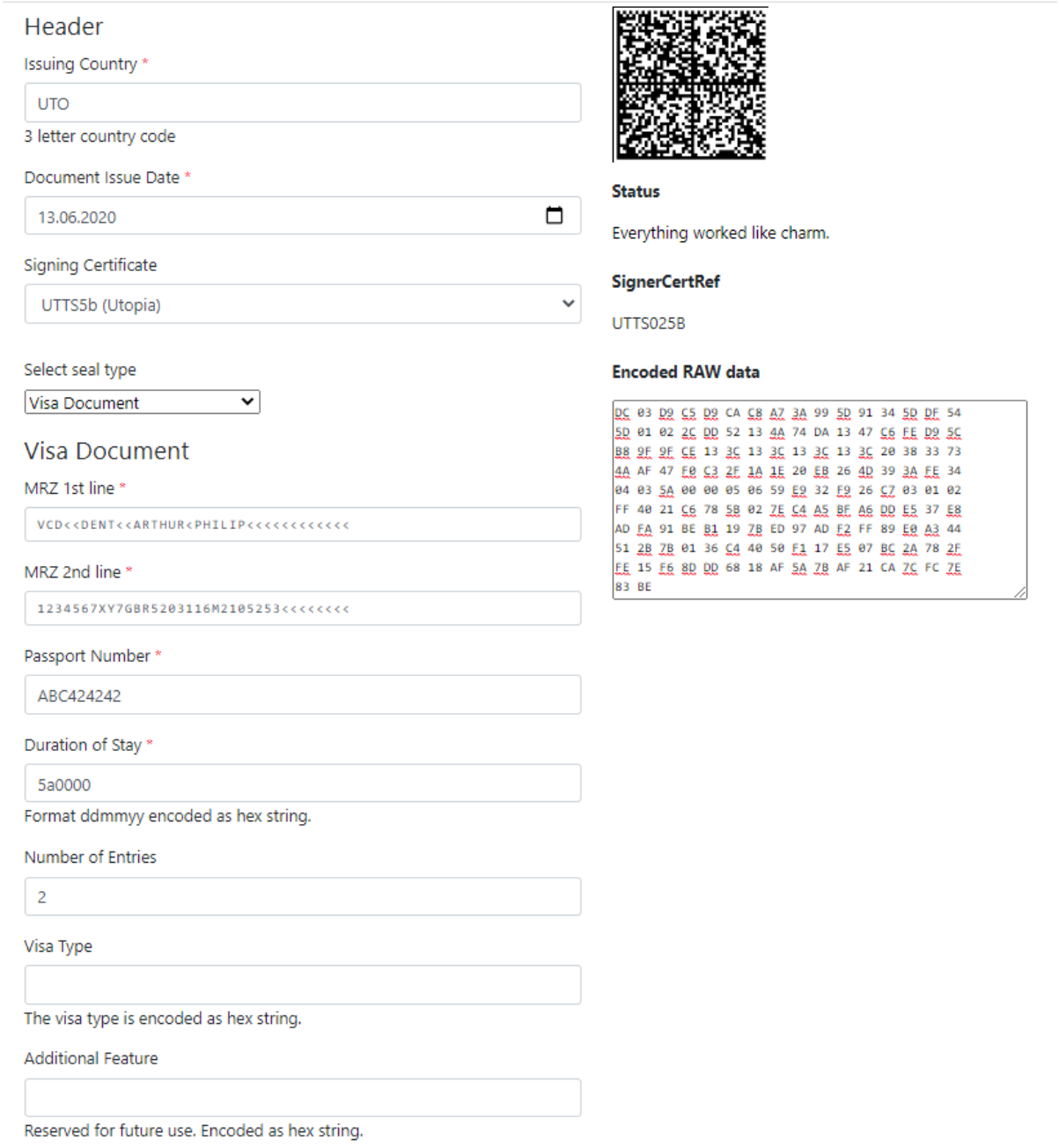


Figure 19: Example Visible Digital Seal for Visa

Suppose that `seal.bin` contains the header and message zone (note that start and length of the signature zone 0xFF and 0x40 are excluded), that the signature is DER encoded in `sig.bin`, and the above PEM encoded private key in `priv_key.pem`. The signature can then be verified with `openssl` by:

```
openssl dgst -sha256 -prverify priv_key.pem -signature sig.bin
- sha256 seal.bin
```

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 20YY

Part 8: Emergency Travel Documents

Approved and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 8 — *Emergency Travel Documents*
Order No.: 9303P8
ISBN 978-92-9258-436-8

DOCUMENT CHANGE RECORD

Doc 9303, Part 8

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

1. SCOPE

This Part 8 of Doc 9303 provides guidance on Emergency Travel Documents (ETDs). The purpose of this guidance material is to promote a consistent approach in the issuance of ETDs in order to:

- enhance the security of the document;
- protect the individual;
- promote greater confidence for border staff in handling ETDs at ports; and
- address the vulnerabilities presented by inconsistent practices and security features.

The guidance material covers travel documents issued by Issuing Authorities to travellers in distressed or unpredicted situations where it is not possible to issue a standard full-validity passport or travel document book and addresses the following areas:

- security/issuance;
- cost;
- format;
- validity;
- document title/name; and
- post-issuance.

This guidance material does not cover:

- standard full-validity passports delivered in emergency situations;
- standard passports delivered with limited validity;
- convention travel documents (which are covered under separate guidance on Issuing Machine Readable Convention Travel Documents for Refugees and Stateless Persons[1]), or “Laissez- passer” issued by the United Nations or the European Union; or
- travel documents issued by humanitarian organizations such as the International Committee of the Red Cross (ICRC).

However, it is intended that this guidance material can be used as a measure of best practice across all issuing organizations, such as humanitarian organizations who issue travel documents to stateless and displaced persons, and vulnerable migrants (including refugees and asylum seekers). Humanitarian organizations are encouraged to comply with its general principles to improve the standards and security of their documents.

Part 8 also specifies the use of Visible Digital Seals in ETDs, an optional feature which if implemented, shall be encoded as specified in this Part 8.

[1] See ICAO/UNHCR Guide for Issuing Machine Readable Convention Travel Documents for Refugees and Stateless Persons.

2. INTRODUCTION

2.1 What is an Emergency Travel Document (ETD)

Emergency travel documents are issued by States to travellers needing to travel urgently in distressed or unpredicted situations where it is not possible to issue a standard full-validity passport.

Where the Issuing Authority considers that the person has a justified need to travel on urgent or compassionate grounds, a State may issue a specific type of document, commonly a passport-sized book (with fewer pages) or, depending on the circumstances outside the country of origin or in the country of issuance, a single sheet, with a restricted time and territorial validity, in order to facilitate scheduled travel back to the country of origin or to a named destination or to complete short-term travel.

The terminology used for documents issued in these situations is confusing, and various terms are used by different Issuing Authorities for the same document.

Some of the terms used are set out below, and it is not always clear what the specific term means:

- emergency passport
- emergency travel document
- emergency travel certificate
- temporary passport
- temporary travel document
- provisional passport
- provisional travel document.

For the purposes of this guidance material, the term Emergency Travel Document (ETD) is used to describe this range of documents. This guidance material has been drafted to provide the flexibility for the Issuing Authority to determine the specific type of document to be issued (a limited-page passport-sized book or a single sheet), which can vary on a case-by-case basis.

It is noted that the majority of Issuing Authorities do not issue ETDs to refugees or stateless persons or to anyone who is not a citizen of their own State/Member State. However, in exceptional, crisis situations, ETDs may be issued, usually in the form of a laissez-passer. As part of the provision of humanitarian aid, organizations such as the ICRC issue travel documents to asylum seekers, refugees, vulnerable migrants, and displaced or stateless persons in emergency situations. Such travel documents are issued for a one-way journey and after the completion of visa and travel requirements. They are issued only as a last resort when Issuing Authorities are not in a position to issue a full-validity passport or travel document.

2.2 Problems arising from a lack of global standards or recommended best practices

A specific ETD in a uniform format[2] is issued by a number of Member States of the European Union to unrepresented EU citizens in third countries (i.e. EU citizens holding the nationality of a Member State which is not represented in a given third country), whose passports have been lost, stolen or destroyed or are temporarily unavailable. The document can be issued by any EU Member State under the authority of the Member State of nationality. It covers a single journey with a

[2] 96/409/CSFP: Decision of the Representatives of the Governments of the Member States, meeting within the Council of 25 June 1996 on the establishment of an emergency travel document.

validity period barely longer than the minimum period required for completion of the journey for which it is issued. The purpose of the common-format EU ETD is to provide genuine assistance to unrepresented EU citizens in emergency situations in third countries. Some EU Member States issue their own national ETDs to unrepresented EU nationals for the same purpose.

However, there were no global standards or recommended practices for the issuance of ETDs. Annex 9 — *Facilitation* of the Convention on International Civil Aviation (the "Chicago Convention"), provides an exemption for ETDs from ICAO minimum standards for MRTDs. As a result, varying standards are used by each individual Issuing Authority. There is no clear definition for ETDs, and they may have a lower security level attached to their deliverance. This can result in:

- ETDs being issued routinely as a (standard) document to travel, especially in the cases where countries have centralized the production and issuance of their national passports to the home country when an application is made overseas (as this process is easier);
- ETDs being targeted by potential fraudsters, considering the ETD's limited security level;
- Issuing Authorities being required to consider documentation that can be variable in terms of security and quality of issue; and
- Other humanitarian organizations that issue travel documents (for example to stateless and displaced persons, or vulnerable migrants including refugees and asylum seekers) not having guidance on issuance or acceptance by which to improve the standards and security of their documents.

2.3 Terminology used

It is recognized that States often issue more than one type of ETD to fulfil varying operational and policy requirements, and the terminology varies considerably. It is also recognized that, as a consequence of specific arrangements, in some cases a single, common-format ETD is issued by a number of States to citizens of any other of the States participating in such arrangements (e.g. the common-format ETD issued to unrepresented citizens of the European Union). Therefore, this guidance material should establish a single name to be used (see also section 4.5).

3. BACKGROUND

The Chicago Convention provides a mandate to develop and maintain Standards and Recommended Practices (SARPs). The Standards and specifications developed are a means of ensuring that inspection authorities have a satisfactory level of confidence in the reliability of travel documents and can use their equipment to process presented travel documents in a globally interoperable manner.

4. PRINCIPLES AND RECOMMENDED PRACTICES

4.1 Security/Issuance

4.1.1 Circumstances to issue ETDs

A traveller may find that he or she is unable to obtain a standard full-validity passport but needs nevertheless to travel urgently. The issuance of an ETD by an Issuing Authority may be considered in relation to but not be limited to the following situations:

- emergency situation for the individual traveller (for example, a family illness; death of a relative) with inadequate time to apply for a standard full-validity passport, including urgent travel needs while a standard full-validity passport has been lost, stolen or damaged/mutilated;
- emergency situation abroad (for example, a conflict or natural disaster such as a flood or earthquake) and a need to travel home;
- lost, stolen or damaged/mutilated passport while abroad;
- contingency arrangements if a standard full-validity passport cannot be issued in-country;
- deportation, removal, repatriation; and
- unrepresented foreign nationals who cannot access their own consular services in case of emergency or are in personal emergency situations (for example, when their documents are lost, stolen, destroyed or inaccessible).

The type of document issued in the above situations may not be the same in all cases. The traveller's situation and the individual circumstances of each case should be taken into account when an Issuing Authority determines which travel document is most appropriate. The criteria for issuing an ETD should be made available on request to the traveller.

ETDs are often issued in locations[3] abroad[4] where it is either impractical or inappropriate for an individual to apply for a standard full-validity passport.

Ultimately, the type of travel document issued is dependent on the individual circumstances, the environment surrounding its issuance, and the practices of an Issuing Authority. In most cases, the security of the document often reflects the circumstances under which the ETDs are issued and the access to facilities and technology available at the time.

4.1.2 Issuance process of ETDs

The issuance process for ETDs should stay as close as possible to that for standard MRTDs. In line with the Annex 9 requirement for transparent processes, Issuing Authorities should define which steps of the issuance process can diverge, and under which circumstances. States of emergency may necessitate issuance of ETDs in less than ideal circumstances and at very short notice so it is important that issuing staff can be assured that they have the most robust process possible (given the circumstances). There may be different ways of achieving enhanced integrity in these situations:

- Verification: It is recommended that the issuers satisfy themselves that proper checks are carried out against Interpol or other national databases wherever possible. Travel documents are only as secure as the identity assurance processes behind their production and issuance.

- Enrolment/Application: It is recommended that details of the ETD application, and of the document issued, are recorded on the applicant's file for future reference. It is important that even (or perhaps especially) in cases of

[3] Emergency travel documents may be issued from a number of locations including but not limited to:

Issuance overseas:
i. from an embassy, high commission or honorary consul.
ii. from a remote area in crisis, (e.g. mobile response unit) where the person issuing the documents must work in tandem with his/her home office to ensure that all required eligibility and security procedures are met.
iii. from airports in crisis situations.
iv. from a designated embassy, high commission or honorary consul of other countries where a special arrangement is in place.

Issuance domestically:
i. from the airport.
ii. from an office of the Issuing Authority.

[4] There are examples of good practice whereby some States have special arrangements with partners to provide emergency services overseas through embassies, high commissions, honorary consuls or trusted third parties (private sector industry) in States where they do not have a presence. Although these partnerships are rare, this guidance material encourages States to explore this option on a bilateral basis.

manual issuance this information forms part of the applicant's case history.

- Entitlement/Identity verification: It is recommended that, where possible, States request supporting identification documents to assist them in their decision to issue an ETD. Additionally, where biometric verification/identification may be used to support identity verification processes, States should make use of this.

- Linking to the standard full-validity passport: Where a standard full-validity passport has previously been issued, it is recommended that States consider linking it to the ETD in order to establish the applicant's case history and provide further identity assurance. This practice will also help ensure that the document is taken out of circulation at the final destination State (see section 4.6 on "post-issuance"). An alert flag may be raised for first-time applicants, where no previous passport record exists. It is advisable to keep record of all travel documents, including any ETDs, over a determined period of time.

- Informing the applicant: It is recommended that the applicant be informed of the need to apply for a standard full-validity passport should he or she wish to travel at a future date. The applicant should also be made aware that Issuing Authorities may retain his or her ETD on arriving at the destination, depending on whether it has been issued for one journey or more than one.

4.1.3 Two types of ETDs

There are two possible options when Issuing Authorities face the need to issue an ETD. Either they consider delivering:

1. a (limited-page) passport-sized booklet; or
2. a single-sheet travel document (normally a stand-alone A4-sized paper sheet or a fold-out document).

The (limited-page) passport-sized booklet should be issued wherever possible and should comply with the relevant specifications in ICAO Doc 9303 relating to MRTDs. The advantages of issuing this type of booklet are:

- The booklet can be personalized in a more secure manner than a single-sheet document;
- It provides greater scope for inclusion of security features;
- It offers more reliability because the inclusion of a Machine Readable Zone (MRZ) will ensure that the document can be swiped through a passport reader and automatically checked against watch lists and other systems;
- It provides a broader acceptance/recognition level by other countries and international parties/entities; and
- It entitles the holder to a wider range of travel options (although limited, the passport-sized document offers a longer validity and more pages than the single-sheet travel document valid for one trip only).

In situations (for example, during a natural disaster or in a conflict situation) where it is not appropriate or practical to issue the (limited page) passport-sized MRTD booklet, it is also possible to produce/issue a single-sheet document. The advantages of issuing a single-sheet document in these types of situations are:

- It may be issued in crisis situations where facilities to personalize a book are inaccessible or unavailable;
- It may be quicker to personalize than the passport-sized book;
- It may be a more cost-effective option; and
- It will be subject to more scrutiny at borders.

4.1.4 Principle

Given the de facto circumstances, the most secure document that can be issued should be issued.[5]

4.1.5 Recommended best practice

- A machine-readable ETD is the preferred standard, primary document.
- ETDs that exist in booklet form should have a limited number of pages (conform to its limited validity) and be consistent with the security features guidance contained in ICAO Doc 9303.
- States shall circulate specimen information to other States and concerned organizations such as airlines, including information on the design, security features and issuance procedures of ETDs[6].
- States should define that no person should hold more than one valid ETD concurrently.
- An ETD should be issued as near to the date of travel as possible to ensure it is used for the specified purpose and exact journey for which it was issued.

In cases where a MRTD ETD is not issued, the single-sheet travel document shall be issued instead, noting that:

- Single-sheet ETDs should contain the minimum, basic security features, such as a watermark, security background printing or UV fluorescence ink or elements so as to counteract fraudsters' actions and to offer an adequate acceptance and recognition level.
- Whenever possible, receiving and/or transiting authorities should be informed about the travel plan of persons holding single-sheet ETDs, so as to ensure proper facilitation procedures (especially in case of transiting ports).
- States shall circulate specimen information to other States and concerned organizations such as airlines, including information on the design, security features and issuance procedures of single-sheet ETDs.
- States should define that no person should hold more than one valid ETD concurrently.
- A single-sheet ETD should be issued as near to the date of travel as possible to ensure it is used for the specified purpose and exact journey for which it was issued.

4.2 Cost

The cost of issuing either type of ETD is a matter for the Issuing Authority, including any requirements on charging and fee waiving in its national legislation. The Issuing Authority should consider the level of charging at a rate that does not encourage the person to apply for an ETD rather than a standard full-validity passport. Also, the charge should be set at a level that discourages holders of standard full-validity passports from not taking sufficient care of their existing passport. The Issuing Authority may consider issuing an ETD free of charge, including in crisis situations (e.g. State of Emergency). Regardless of cost, in all cases the ETD should be issued only when all relevant checks have been completed.

4.2.1 Principle

The charging structure within national frameworks for issuing ETDs should be clear, and applicants should be aware of the cost that will be applied.

[5] Issuing Authorities may consider issuing a less secure document in conjunction with the receiving and/or transiting Authorities if the circumstances merit and justify this.

[6] Reference can be found on www.icao.int/security/fal/trip - "Guide for Circulating Specimen Travel Documents"

4.2.2 Recommended best practice

In the circumstances of a national or local crisis, the granting of an ETD may be free of charge.

4.3 Format

While there will always be the potential for situations to arise where it is impossible to produce the passport-sized machine-readable booklet form of the ETD, this is to be regarded as the preferred standard primary document. Issuing Authorities should issue the most secure document that can be issued in the circumstances, while meeting all entitlement and security requirements. It is crucial that Issuing Authorities ensure the highest security level possible to deter fraudulent use.

4.3.1 Principle

The document, if in booklet form, should be easily distinguishable from a standard full-validity passport but, as set out below, some format, security and design features should remain identical.

4.3.2 Recommended best practice

Issuing Authorities should issue an ETD in a form that clearly distinguishes it from a standard full-validity passport. This may be a different coloured cover and inner pages or the cover and pages might be the same but with an additional marking clearly indicating that they are different. It is recommended though that, for ease of recognition by border control authorities, a link be kept to the current standard passport.

- It is recommended that there be fewer pages than in a standard full-validity passport to reflect the fact that these are short-term documents, preferably with a maximum of eight (8) visa/ inner pages.
- In accordance with Doc 9303, for the booklet form of the ETD, the photo, whether provided in paper or digital format, must be digitally printed in the ETD. Necessary measures shall be taken by the Issuing Authority or organization to ensure that the displayed photo is resistant to forgery and substitution.
- Stick-on photos are not permitted in accordance with Doc 9303[7] in the booklet form of the ETD due to the ease with which stick-on photos can be removed. Given that ETDs may not contain the same or as many security safeguards or features as a standard full-validity passport, steps need to be taken to protect the ETD wherever possible. Consequently, the integration and printing of the photo into the ETD booklet should be a standard requirement given the widespread recognition of the weakness of stick-on photos.
- The ETD should have a unique number printed pre-issuance which will enable an audit trail of which documents were issued to whom. This can be particularly important when documents are lost or stolen, either pre- or post-issuance.
- To the extent possible single-sheet ETDs should incorporate and assimilate the same principle and best practices, noting that, where stick-on photos need to be used, Issuing Authorities should consider using sticker/vignette laminates, or wet and/or dry stamps on the single-sheet ETDs as a mitigating practice and to increase security.

[7] In line with Doc 9303-4: “The use of affixed or stick-on portrait photos is not permitted and these shall not be used. Instead, the portrait image shall be integrated with the bio data page using a secure personalization technology.”

4.4 Validity

ETDs are issued for a variety of reasons, and it is no longer the case that they are used only for single journeys from one country back to the country of nationality, citizenship or residence. Many countries insist upon travellers having at least six (6) months' validity in their travel documents in order to issue visas or give leave to enter.

4.4.1 Principle

Issuing Authorities should restrict validity to the minimum period required consistent with the purpose for which the document was issued and in line with the security of the document.

4.4.2 Recommended best practice

- ETDs in booklet form should be issued with an absolute maximum validity of twelve (12) months (including any six-month entry and visa requirements).
- Single-sheet ETDs should be issued with a single journey restriction (which can include transit points).
- All ETDs should have final destinations and fixed named transit points on the document, and these should reflect the ticketed route.
- All ETDs should be replaced by a standard full-validity passport as soon as possible. (If time allows preferably during the validity of the ETD.)

4.5 Document title/name

In order to avoid confusion, the single term of "Emergency Travel Document (ETD)" should be used to describe this range of documents. This best reflects the idea of a distressed and unpredicted situation in an unequivocal manner. It thus mirrors the notions of urgent, critical, short-term and transitory.

The term is also broad enough to be seen in the context of two different existing ETDs: a booklet format and a single-sheet format. For the single-sheet ETD the words "single journey" should be inserted in the "validity" box.

4.5.1 Principle

Issuing States or organizations should use a distinctive title or name on the ETDs so as to clearly identify the distressed and unpredicted situations in which such documents were issued (and to distinguish them from documents issued in situations where States choose to issue a regular passport or travel document book with limited validity, i.e., a temporary passport).

4.5.2 Recommended best practice

- ETDs regardless of their format should be referred to as "Emergency Travel Documents" to clearly distinguish ETDs from standard full-validity passports and should include the word "Emergency" in the title.
- They can be issued in booklet or single-sheet format.
- In case of the single-sheet format, they should mention "single journey" in the "validity" box.

4.6 Post-issuance

The practices for resolving used ETDs with issuance systems vary widely, particularly depending on whether or not documents need to be retained by the traveller in order to collect a standard full-validity passport, and also depending on whether ETDs are issued by a different ministry or department from that issuing standard full-validity passports.

4.6.1 Principle

Issuing States or organizations should take specific measures to prevent further use of post-use ETDs to minimize the chances of potential fraud.

4.6.2 Recommended best practice

The document should be taken out of circulation at the border crossing point of the final destination, unless explicitly required or noted on the document by the Issuing Authorities.[8] The document should ultimately be returned to the Issuing Authorities for physical cancellation and/or mutilation to prevent it being used for further travel by impostors or fraudsters.

5. SUMMARY

The table below aims to emphasize the key drivers and the purpose for producing this guidance material, summarizing the scope, principles and best practice recommendations encompassed within it.

<table>
<tr><td colspan="3">KEY DRIVERS: To help promote security and improve traveller facilitation by:
• minimizing fraud;
• preventing potentially dangerous people from traveling;
• removing potential vulnerabilities of Issuing Authorities.</td></tr>
<tr><td colspan="3">PURPOSE: To promote a consistent approach in the issuance of ETDs in order to:
• enhance the security of the document;
• protect the individual;
• promote greater confidence for border staff in handling ETDs at ports;
• address the vulnerabilities presented by inconsistent practices and security features.</td></tr>
<tr><td>Scope</td><td>Principles</td><td>Recommended best practices</td></tr>
<tr><td>Security/ Issuance</td><td>1. Given the de facto circumstances, the most secure document that can be issued should be issued.</td><td>i. A machine-readable ETD is the preferred standard, primary document.
ii. ETDs that exist in booklet form should have a limited number of pages (conform to its limited validity) and be consistent with the security features guidance contained in ICAO Doc 9303.
iii. States shall circulate specimen information to other States and concerned organizations such as airlines, including information on the design, security features and issuance procedures of ETDs.
iv. States should define that no person should hold more than one valid ETD concurrently.</td></tr>
</table>

[8] For example, visa requirements (e.g. if an expired travel document contains a valid visa, the travel document, after invalidation, stays with its rightful holder).

		v. An ETD should be issued as near to the date of travel as possible to ensure it is used for the specified purpose and journey for which it was issued. vi. In cases where a MRTD ETD is not issued, the single-sheet travel document shall be issued instead, noting that: vii. Single-sheet ETDs should contain minimum, basic security features, such as a watermark, security background printing or UV fluorescence ink or elements so as to counteract fraudsters' actions and to offer an adequate acceptance and recognition level; viii. Whenever possible, receiving and/or transiting authorities should be informed about the travel plan of persons holding single-sheet ETDs, so as to ensure proper facilitation procedures (especially in case of transiting ports); ix. States shall circulate specimen information to other States and concerned organizations such as airlines, including information on the design, security features and issuance procedures of single-sheet ETDs; x. States should define that no person should hold more than one valid ETD concurrently; xi. A single-sheet ETD should be issued as near to the date of travel as possible to ensure it is used for the specified purpose and journey for which it was issued.
Cost	2. The charging structure within national frameworks for issuing ETDs should be clear and applicants should be aware of the cost that will be applied.	xii. In the circumstances of a national or local crisis, the granting of an ETD may be free of charge.
Format	3. The document, if in booklet form, should be easily differentiated from a standard full-validity passport but some format, security and design features should remain identical.	xiii. Issuing Authorities should issue ETDs in a form that clearly distinguishes them from standard full-validity passports. This may be a different coloured cover and inner pages or the cover and pages might be the same but with an additional marking clearly indicating that they are different. xiv. It is recommended though that, for ease of its recognition by border control authorities, a link be kept to the current standard passport.

		xv. It is recommended that there be fewer pages than in a standard full-validity passport to reflect the fact that these are short-term documents, preferably with a maximum of 8 visa/inner pages. xvi. In accordance with Doc 9303, for the booklet form of the ETD, the photo, whether provided in paper or digital format, must be digitally printed in the MRTD. Necessary measures shall be taken by the Issuing Authority or organization to ensure that the displayed photo is resistant to forgery and substitution. xvii. For the booklet form, stick-on photos are not permitted in accordance with Doc 9303 due to the ease with which they can be removed. Given that ETDs may not contain the same or as many security safeguards or features as a standard full-validity passport, steps need to be taken to protect the ETD wherever possible. Consequently, the integration and printing of the photo into the ETD booklet should be a standard requirement given the widespread recognition of the weakness of stick-on photos. xviii. The ETD should have a unique number printed pre-issuance to enable an audit trail of which documents were issued to whom. This can be particularly important where documents are lost or stolen, either pre- or post-issuance. xix. To the extent possible, single-sheet ETDs should incorporate and assimilate the same principle and best practices, noting that, where stick-on photos need to be used, Issuing Authorities should consider using sticker/ vignette laminates, or wet and/or dry stamps on the single-sheet ETDs as a mitigating practice and to increase security.

Validity	4. Issuing Authorities should restrict validity to the minimum period required, consistent with the purpose for which the document was issued and in line with the security of the document.	xx. ETDs in booklet form should be issued with an absolute maximum validity of 12 months (including any six-month entry and visa requirements). xxi. Single-sheet ETDs should be issued with a single journey restriction (which can include transit points). xxii. All ETDs should have final destinations and fixed named transit points on the document, and these should reflect the ticketed route. xxiii. All ETDs should be replaced by a standard full-validity passport as soon as possible (if time allows preferably during the validity of the ETD) with the standard robust application process being followed.
Document title/name	5. Issuing States or organizations should use a distinctive title or name on the ETDs so as to clearly identify the distressed and unpredicted situations in which such documents were issued (and to distinguish them from documents issued in situations where States choose to issue a regular passport or travel document book with limited validity, i.e., a temporary passport).	xxiv. ETDs, regardless of their format, should be referred to as “Emergency Travel Documents” to clearly distinguish ETDs from standard full-validity passports and should include the word “Emergency” in the title. xxv. They can be issued in booklet or single-sheet format. xxvi. In case of the single-sheet format, they should mention “single journey” in the “validity” box.
Post-issuance	6. Issuing States or organizations should take specific measures to prevent further use of post-use ETDs to minimize the chances of potential fraud.	xxvii. The document should be taken out of circulation at the border crossing point of the final destination, unless explicitly required or noted on the document by the Issuing Authorities. The document should ultimately be returned to the Issuing Authorities for physical cancellation and/or mutilation to prevent it from being used for further travel by impostors or fraudsters.

6. USE OF OPTIONAL VISIBLE DIGITAL SEALS FOR ETDS

This section specifies the profile for digital seals in ETDs.

A Visible Digital Seal (VDS) is a 2D barcode that includes a cryptographically signed data structure, which can be printed on a non-electronic document to increase its security. Doc 9303-13 specifies VDS for non-electronic documents.

Considering the ETD's limited security level compared to eMRTDs, they are being targeted by potential fraudsters. Digital seals are a means to ensure the integrity and authenticity of ETD data in situations where it is not possible to issue a standard full validity passport or other regular travel documents. A worked example for the MRZ of an ETD is described in Appendix A.

6.1 Content and Encoding Rules

6.1.1 Header

The *Document Feature Definition Reference* for this use-case is `0x5E`.
The *Document Type Category* for ETDs is `0x03`.
Otherwise, the content of the header is the same as defined in Doc 9303-13.

6.1.2 Document Features of a digital seal for ETDs

For the document feature set including only the MRZ as below, the *Document Feature Definition Reference* value is `94dec`.

Machine Readable Zone (REQUIRED)

Basic Information are encoded using a Machine Readable Zone (MRZ) of a TD2-Format MROTD, see Doc 9303-6. The MRZ of ETDs contains the following information:

- document code;
- issuing state or organization;
- primary and secondary identifiers of the document holder;
- document number;
- nationality of the document holder;
- date of birth of the document holder;
- sex of the document holder; and
- date of expiry.

Additional Document Features (Future use)

In future versions of this specification additional (OPTIONAL and/or REQUIRED) feature fields may be defined. In case additional fields are present, a new unique Document Feature Definition Reference MUST be assigned for each combined set of OPTIONAL and REQUIRED feature fields.

6.1.3 Encoding Rules for Document Features

In the following, the digital encoding of document features of the ETD seal is defined.

MRZ (TD2-Type Doc 9303, Part 6: Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs))

Tag:	0x02
Min. Length:	48 Byte
Max. Length:	48 Byte
Value Type:	Alphanumeric
Required:	Required
Content:	The first line and second line of the MRZ of a TD2-MROTD (2*36 chars.). The filler symbol < in the MRZ is replaced by <SPACE> prior to encoding by C40.

6.1.4 Signature

Appropriate key lengths offering protection against attacks SHALL be chosen for the hashing and signature algorithms. Suitable cryptographic catalogues SHOULD be taken into account.

6.2 Bar Code Signer and Seal Creation

A possible architecture and implementation for the ETD signer and its client is described in Doc 9303-13. For the security of the ETD signing system, see Doc 9303-13.

6.3 Public Key Infrastructure (PKI) and Certificate Profiles

For the ETD, the requirements which are mentioned in Doc 9303-12 apply. The following deviations are given for the specific ETD profile.

6.3.1 Key Requirements (Validity Period)

ETD-Signer Certificates

Private Key Usage Time:	1 year + 2 month (the 2 month are meant for smooth roll-over)
Certificate Validity:	Private Key Usage Time + ETD Validity Timeframe

7. REFERENCES (NORMATIVE)

Annex 9 Convention on International Civil Aviation (“Chicago Convention”), Annex 9 – *Facilitation.*

APPENDIX A TO PART 8 —ETD VALIDATION POLICY RULES (INFORMATIVE)

The Validation Policy Rules outlined in Doc 9303-13 apply. In addition to these rules, there are further validation rules for the ETD which are described in the following paragraphs.

In addition to the generic document Validation Policy, the policy for ETDs considers the following questions:

1. Is the MRZ printed on the ETD valid?
2. Does the MRZ of the ETD match with the MRZ stored in the digital seal?

Further validation steps (e.g. utilizing additionally encoded data) are out of scope of this profile. Outlined below are ETD specific validation rules for each type of control, list the validation criteria, expected results for each criteria, and resulting status sub-indications.

Visible Digital Seal Validation

1. Format Validation

2. Digital Seal MRZ Validation
   - if the checksums of the MRZ stored in the seal are not compliant/valid then the status is INVALID with sub-indication INVALID_SEAL_MRZ

If all checks above do not result in INVALID and the reader is not capable of OCRing the printed MRZ, the status is VALID. If the reader is capable of OCRing the printed MRZ, the next checks MUST be conducted:

3. Printed MRZ Validation (depending on reader capability)
   - if the checksums of the OCRed, printed MRZ are not compliant/valid then the status is INVALID with sub-indication INVALID_PRINTED_MRZ
   - if the checksums of the OCRed, printed MRZ is compliant/valid then compare the printed MRZ character by character with the MRZ stored in the seal (note that for storing the MRZ in the seal, the filler character '<' is replaced by <SPACE>. If any characters mismatch, then the status is INVALID with sub-indication SEAL_DOCUMENT_MISMATCH.
   - Otherwise, the result is VALID.

   The above step covers a comparison of the data stored in the seal against data stored on the MRZ of the document. If an automatic check is impossible since the printed data of the document cannot be OCRed during validation, a manual inspection should be conducted by comparing the printed MRZ with the one stored in the (valid) seal.

Table A1: Trust Levels of the ETD Policy

Status Indication	Sub Status Indication	Trust Level
INVALID	INVALID_SEAL_MRZ	*high fraud potential*
	INVALID_PRINTED_MRZ	
	SEAL_DOCUMENT_MISMATCH	

APPENDIX B TO PART 8 —WORKED EXAMPLE VISIBLE DIGITAL SEAL FOR ETD (INFORMATIVE)

The following example shows a visible digital seal (VDS). To generate the signature ECDSA256 with the curve brainpool256r1 must be used. This example only contains the header and data of the document.

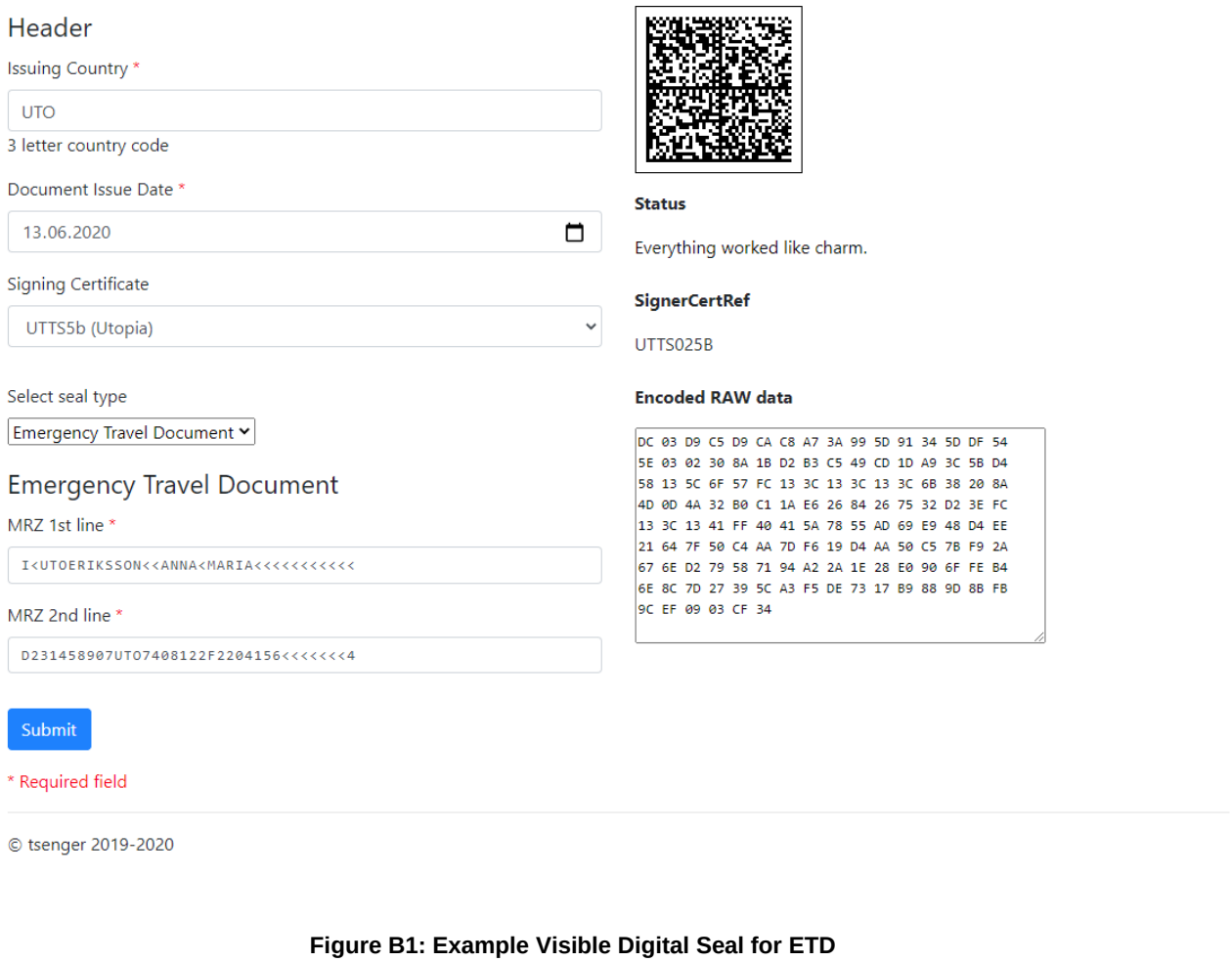


Figure B1: Example Visible Digital Seal for ETD

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 202x

Part 9: Deployment of Biometric Identification
and Electronic Storage of Data in MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 9 — *Deployment of Biometric Identification and Electronic Storage of Data in MRTDs*
Order No.: 9303P9
ISBN 978-92-9249-797-2

DOCUMENT CHANGE RECORD

Doc 9303, Part 9

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

1. SCOPE

Part 9 of Doc 9303 defines the specifications, additional to those for the basic MRTD set forth in Parts 3, 4, 5, 6, and 7 of Doc 9303, to be used by States or organizations wishing to issue an electronic Machine Readable Travel Document (eMRTD) capable of being used by any suitably equipped receiving State or organization to read and to authenticate data relating to the eMRTD itself and verification of its holder. This includes mandatory globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems. The specifications require the globally interoperable biometric data to be stored in the form of high-resolution images on a high-capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. The specifications also permit the storage of a range of optional data at the discretion of the issuing State or organization. Since the use of the contactless IC is independent of the size of the document, all specifications apply to all eMRTD sizes in their electronically enabled form. Differences between eMRTD formats relate to the MRZ, with consequences for the storage of the MRZ in the contactless IC. These differences are indicated in the specifications of the Logical Data Structure in Doc 9303-10.

Part 9 shall be read in conjunction with:

- Part 1 — Introduction;
- Part 10 — Logical Data Structure (LDS);
- Part 11 — Security Mechanisms for MRTDs;
- Part 12 — Public Key Infrastructure for MRTDs.

2. eMRTD

Note.— The terms MRTD and eMRTD are used in this document as a generic reference to all types of Machine Readable Travel Documents in, respectively, optical character reading and electronically enabled forms. The terms TD1, TD2 and TD3 refer to the different form factors of MRTDs. All eMRTDs referred to in this Part are electronically enabled.

2.1 Conformance to Doc 9303

An electronic MRTD (eMRTD) SHALL conform in all respects to the specifications provided in Doc 9303.

2.2 Validity Period for an eMRTD

The validity period of an eMRTD is at the discretion of the issuing State or organization; however, in consideration of the limited durability of documents and the changing appearance of the document holder over time, a validity period of not more than ten years is RECOMMENDED. One MAY wish to consider a shorter period to enable the progressive upgrading of the eMRTD as the technology evolves.

2.3 Chip Inside Symbol

Doc 9303-9 focuses on biometrics in relation to Machine Readable Travel Documents, using the term “eMRTD” to denote such biometrically-enabled and globally-interoperable MRTD. Any MRTD that does not comply with the specifications given in Doc 9303 may not be called an eMRTD and shall not display the Chip Inside symbol.

All eMRTDs shall carry the following symbol:

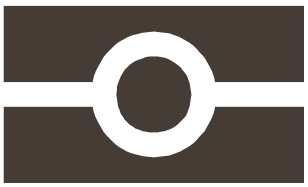


Figure 1. Chip Inside symbol

An electronic file of the symbol is available from the ICAO website. The symbol SHALL only appear on an eMRTD that contains a contactless integrated circuit, with a data storage capacity storage capacity sufficient to hold the mandatory data elements in accordance with the Logical Data Structure (Doc 9303-10), with all entered data secured with a digital signature as specified in Doc 9303-11. Unless an eMRTD conforms to these minimum requirements, it SHALL NOT be described as an eMRTD nor display the Chip Inside symbol. The symbol shall appear on the front cover of the eMRTD if it is a TD3 size book (eMRP) either near the top or the bottom of the cover, or on the front side of the eMRTD if it is in the format of a card (eMROTD).

On an eMRP the symbol shall be included in the foil blocking or other image on the front cover. It is recommended that the symbol also be printed on the data page in a suitable colour and in a location which does not interfere with the reading of other data. The issuing State or organization may also print the symbol on the inside page or cover of the passport book that contains the contactless IC and, at its discretion, elsewhere in the passport.

On an eMROTD the symbol SHALL appear on the front of the eMROTD preferably in Zone I.

The image, as shown in Figure 1, is a positive, i.e. the black part of the image shall be printed or otherwise imaged. It is RECOMMENDED that the symbol appears eye-visible and is easily recognizable.

Figure 2 shows the RECOMMENDED dimensions of the symbol as it is to appear on an eMRP cover or data page, or on an electronic TD2.

A smaller size of 4.2 × 7.2 mm (0.17 × 0.28 in), scaled in proportion, is RECOMMENDED for use on an electronic TD1.

The symbol MAY be scaled in proportion for use in, for example, background designs.

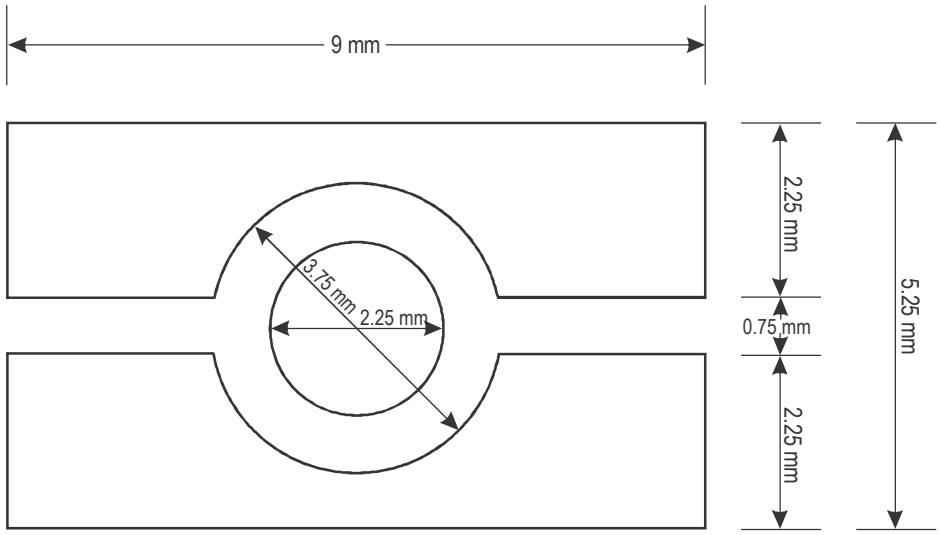


Figure 2. Dimensions of the symbol

Note.— The following are the corresponding dimensions in inches: 9.0 mm (0.35 in), 5.25 mm (0.21 in), 3.75 mm (0.15 in), 2.25 mm (0.09 in), 0.75 mm (0.03 in).

2.4 Warning regarding Care in Handling an eMRP

It is suggested that a warning be placed in an obvious location on the book urging the holder of an eMRP to take care of the document. A suggested wording is:

“This passport contains sensitive electronics. For best performance please do not bend, perforate or expose to extreme temperatures or excess moisture”.

In addition, the issuing State or organization may mark the part of the page containing the IC and the corresponding parts of some adjacent pages with the caveat:

“Do not stamp here”.

3. BIOMETRIC IDENTIFICATION

“Biometric identification” is a generic term used to describe automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits.

A “biometric template” is a machine-encoded representation of the trait created by a computer software algorithm and enables comparisons (matches) to be performed to score the degree of confidence that separately recorded traits identify (or do not identify) the same person. Typically, a biometric template is of relatively small data size; however, each manufacturer of a biometric system uses a unique template format, and templates are not interchangeable between systems. To enable a State or organization to select a biometric system that suits its requirements, the data have to be stored in a form from which its system can derive a template. This requires that the biometric data be stored in the form of one or more images.

3.1 ICAO Vision on Biometrics

The ICAO vision for the application of biometrics technology encompasses:

- specification of a primary interoperable form of biometrics technology for use at border control (verification, watch lists) as well as by carriers and document issuers, and specification of agreed supplementary biometric technologies;
- specification of the biometrics technologies for use by document issuers (identification, verification and watch lists);
- capability of data retrieval for 10 years, the maximum recommended validity for a travel document;
- having no proprietary element thus ensuring that any States or organizations investing in biometrics are protected against changing infrastructure or changing suppliers.

Doc 9303 considers only three types of biometric identification systems. With respect to the storage of these three biometric features in the contactless IC of an eMRTD, the issuing State or organization SHALL conform to the relevant international standard.

The types of biometrics are:

- facial recognition – REQUIRED;
- fingerprint recognition – OPTIONAL;
- iris recognition – OPTIONAL.

ISO/IEC 39794 succeeded ISO/IEC 19794:2005 as international standard for encoding biometrics. The following transition time table has been defined:

- Passport reader equipment MUST be able to handle ISO/IEC 39794 data by 2025-01-01 after a five years preparation period starting 2020-01-01.
- Between 2025 and 2030, passport issuers can use the data formats specified in ISO/IEC 19794-X:2005 or in ISO7IEC 39794-X during a five years transition period. During this transition period, interoperability and conformity testing will be essential.
- From 2030-01-01 on, passport issuers MUST use ISO/IEC 39794-X for encoding biometric data.

ISO/IEC 49794 provides guidance on the transition from ISO/IEC 19794:2005 to ISO/IEC 39794.

Biometrics terms

The following terms are used in biometric identification:

- “verify” means to perform a one-to-one match between proffered biometric data obtained from the eMRTD holder now and a biometric template created when the holder enrolled in the system;
- “identify” means to perform a one-to-many search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

Biometrics can be used in the identification function to improve the quality of the background checking performed as part of the passport, visa or other travel document application process, and they can be used to establish a positive match

between the travel document and the person who presents it.

For the purposes of this document, the terms and definitions of the biometrics vocabulary given in ISO/IEC ISO/IEC 2382-37 apply.

3.2 Key Considerations

In specifying biometric applications for eMRTDs, key considerations are:

- *Global Interoperability* — the crucial need to specify a system for deployment to be used in a universally interoperable manner;

- *Uniformity* — the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by issuing States or organizations ;

- *Technical Reliability* — the need to provide guidelines and parameters to ensure issuing States or organizations deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States or organizations reading data encoded by other issuing States or organizations can be sure that the data supplied to them are of sufficient quality and integrity to enable accurate verification in their own system;

- *Practicality* — the need to ensure that recommended standards can be made operational and implemented by States or organizations without their having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards;

- *Durability* — the requirement that the systems introduced will last the recommended maximum 10-year life of a travel document, and that future updates will be backward compatible.

3.3 Key Processes with respect to Biometrics

The major components of a biometric system are:

- *Establish identity* — ensuring that the identity of the enrollee is known without doubt;

- *Capture* — acquisition of a raw biometric sample;

- *Extract* — conversion of the raw biometric sample data to an intermediate form;

- *Create template* — conversion of the intermediate data into a template;

- *Compare* — comparison with the information in a stored reference template.

These processes involve:

- The *enrollment* process is the *capture* of a raw biometric sample. It is used for each new person (potential eMRTD holder) taking biometric image samples for storage. This capture process is the automatic acquisition of the biometric via a capture device such as a fingerprint scanner, photograph scanner, live-capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process — for example, standard pose

facing the camera straight-on for a facial recognition capture; whether fingerprints are captured flat or rolled; eyes fully open for iris capture. The resulting image is compressed and then stored for future confirmation of identity.

- The *template creation* process preserves the distinct and repeatable biometric features from the captured biometric image and generally uses a proprietary software algorithm to extract a template from the stored image. This defines that image in a way that it can subsequently be compared with another sample image captured at the time identity confirmation is required and a comparative score determined. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. Quality standards need to be as high as possible since all future checks are dependent on the quality of the originally captured image. If the quality is not acceptable, the *capture* process should be repeated.

- The *identification* process takes the template derived from the new sample and compares it to templates of enrolled end users to determine whether the end user has enrolled in the system before, and if so, whether in the same identity.

- The *verification* process takes the new sample of an eMRTD holder and compares it to a template derived from the stored image of that holder to determine whether the holder is presenting in the same identity.

3.4 Applications for a Biometric Solution

The key application of a biometrics solution is the identity verification of relating an eMRTD holder to the eMRTD he[1] is carrying.

There are several typical applications for biometrics during the enrolment process of applying for an eMRTD.

The end user's biometric data generated by the enrolment process can be used in a search of one or more biometric databases (identification) to determine whether the end user is known to any of the corresponding systems (for example, holding an eMRTD under a different identity, having a criminal record, holding an eMRTD from another State or organization).

When the end user collects the eMRTD (or presents himself for any step in the issuance process after the initial application is made and the biometric data are captured) his biometric data can be taken again and verified against the initially captured biometric data.

The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

There are also several typical applications for biometrics at the border.

Each time a traveller (i.e. eMRTD holder) enters or exits a State, his identity can be verified against the image created at the time his travel document was issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any Advance Passenger Information (API) system. An issuing State or organization may find it desirable to store the biometric template or templates on the travel document along with the image,

1. Throughout this document, the use of the male gender should be understood to include male and female persons.

so that a traveller's identity can be verified in domestic locations where the biometric system is under the issuer's control.

Two-way check — The traveller's current captured biometric image data, and the biometric data from his travel document (or from a central database), can be matched (if applicable by constructing biometric templates of each) to confirm that the travel document has not been altered.

Three-way check — The traveller's current captured biometric image data, the biometric data from his travel document, and the biometric data stored in a central database can be matched (if applicable by constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person and his eMRTD with the database recording the data that were put in that eMRTD at the time it was issued.

Four-way check — A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the three-way check with the digitized photograph on the data page of the traveller's eMRTD.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States and organizations should also have regard to, and set their own criteria in regard to:

- accuracy of the biometric matching functions of the system. Issuing States or organizations must encode the facial image, and optionally one or more fingerprint or iris biometrics on the eMRTD as per LDS specifications. (The biometric may also be stored on a database accessible to the receiving State or organization). Given an ICAO-standardized biometric image, receiving States or organizations must select their own biometric verification software and determine their own biometric scoring thresholds for identity verification acceptance rates and referral of impostors.
- throughput (e.g. travellers per minute) of either the biometric system or the border-crossing system as a whole.
- suitability of a particular biometric technology (face or finger or eye) to the border-crossing application.

3.5 Constraints on Biometric Solutions

It is recognized that implementation of most biometrics technologies is subject to further development. Given the rapidity of technological change, any specifications (including those herein) must allow for, and recognize there will be, changes resulting from technology improvements.

The biometrics information stored on travel documents shall comply with any national data protection laws or privacy laws of the issuing State or organization.

4. THE SELECTION OF BIOMETRICS APPLICABLE TO eMRTDs

It has long been recognized that name and reputation are not sufficient traits to guarantee that the holder assigned a travel document (eMRTD) by the issuing State or organization is the person at a receiving State or organization purporting to be that same holder.

The only method of relating the person irrevocably to his travel document is to have a physiological characteristic, i.e. a biometric, of that person associated with his travel document in a tamper-proof manner.

4.1 Primary Biometric: Facial Image

Encoding of reference face images

The face portrait printed on the ICAO compliant MRTD is an essential element of that document and one of the most important information carriers binding the document to the holder. A standardized face portrait produced at a high quality helps issuing agencies to screen identity and border agencies to inspect the travel document manually or via automated processing. Requirements to capture and encoding of face images are specified in ISO/IEC 39794-5, Annex D.1.

4.2 Optional Additional Biometrics

Issuing States or organizations optionally can provide additional data input to their (and other States') identity verification processes by including multiple biometrics in their travel documents, i.e. a combination of face and/or fingerprint and/or iris. This is especially relevant where States or organizations may have existing fingerprint or iris databases in place against which they can verify the biometrics proffered to them, for example, as part of an ID card system.

Storage of an optional fingerprint biometric

There are three classes of fingerprint biometric technology: finger image-based systems, finger minutiae-based systems, and finger pattern-based systems. Whilst standards have been developed within these classes to make most systems interoperable amongst their class, they are not interoperable between classes. Three standards for fingerprint interoperability are therefore emerging: storage of the image data, storage of the minutiae data and storage of the pattern data. Where an issuing State or organization elects to provide fingerprint data in its eMRTD, the storage of the fingerprint image is mandatory to permit global interoperability between the classes. The storage of an associated template is optional at the discretion of the issuing State or organization.

When an issuing State or organization elects to store fingerprint image(s) on the contactless IC, the optimal image size SHOULD be be adequate for 1:1 verification.

Requirements to capture and encoding of finger images are specified in ISO/IEC 39794-4.

Storage of an optional iris biometric

Where an issuing State or organization elects to provide iris data in its eMRTD, the storage of the iris image is mandatory to permit global interoperability. The storage of an associated template is optional at the discretion of the issuing State or organization.

When an issuing State or organization elects to store iris image(s) on the contactless IC, the optimal image size SHOULD be adequate for 1:1 verification.

Requirements to capture and encoding of iris images are specified in ISO/IEC 39794-6.

5. STORAGE OF THE BIOMETRIC AND OTHER DATA IN A LOGICAL FORMAT IN A CONTACTLESS IC

It is REQUIRED that digital images be used and that these be electronically stored in the travel document.

5.1 Characteristics of the Contactless IC

A high-capacity contactless IC SHALL be the electronic storage medium specified by ICAO as the capacity expansion technology for use with eMRTDs in the deployment of biometrics.

Contactless IC and encoding

The contactless ICs used in eMRTDs SHALL conform to ISO/IEC14443 Type A or Type B and [ISO/IEC 7816-4]. The LDS SHALL be encoded according to the Random Access method. The read range (achieved by a combination of the eMRTD and the reader) typically is up to 10 cm as noted in [ISO/IEC 14443]. An ISO/IEC 14443 application profile for MRTDs is provided in Doc 9303-10.

Data storage capacity of the contactless IC

The data storage capacity of the contactless IC is at the discretion of the issuing State or organization but SHALL be large enough to store the mandatory stored facial image, the duplicate MRZ data and the necessary elements for securing the data. The storage of additional facial, fingerprint and/or iris images may require a significant increase in data storage capacity. There is no maximum contactless IC data capacity specified.

Storage of other data

An issuing State or organization MAY use the storage capacity of the contactless IC in an eMRTD to expand the machine readable data capacity of the eMRTD beyond that defined for global interchange. This can be for such purposes as providing machine readable access to breeder document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

5.2 Logical Data Structure

To ensure global interoperability for machine reading of stored details, a Logical Data Structure (LDS) defining the format for the recording of details in the contactless IC MUST be adhered to.

Structure of the stored data

The Logical Data Structure is specified in Doc 9303-10. Doc 9303-10 describes in detail the mandatory and optional information to be included within specific biometric data blocks within the LDS.

Minimum data items to be stored in the LDS

The minimum mandatory items of data to be stored in the LDS on the contactless IC SHALL be a duplication of the Machine Readable Zone data in Data Group 1 and the holder's facial image in Data Group 2. In addition, the IC in a compliant eMRTD SHALL contain the Security Object (EF.SOD) that is needed to validate the integrity of data created by the issuer — this is stored in Dedicated File No 1 as specified in the LDS (see Doc 9303-10). The Security Object (EF.SOD) consists of the hashes of the Data Groups in use.

5.3 Security and Privacy of the Stored Data

Both the issuing and any receiving States or organizations need to be satisfied that the data stored on the contactless IC have not been altered since they were recorded at the time of issue of the document. In addition, the privacy laws or practice of the issuing State or organization may require that the data cannot be accessed except by an authorized person or organization. Accordingly ICAO has developed specifications in Doc 9303-11 and Doc 9303-12 regarding the application and usage of modern encryption techniques, particularly Public Key Infrastructure (PKI) schemes, which MUST be used by issuing States or organizations in their Machine Readable Travel Documents made in accordance with Doc 9303. The

intent is primarily to augment security through automated means of authentication of eMRTDs and their legitimate holders internationally. In addition, methods are recommended to implement international eMRTD authentication and to provide a path to the use of eMRTDs to facilitate biometric or e-commerce applications. The specifications in Doc 9303-11 permit the issuing State or organization to protect the stored data from unauthorized access by the use of Access Control.

This edition of Doc 9303 is based on the assumption that LDS1 data will not be written to the contactless IC after personalization. Therefore the personalization process SHALL lock the contactless IC as a final step. Once the contactless IC has been locked (after personalization and before issuance) further data can only be written to the contactless IC after successful execution of an authentication mechanism (TA), as specified in Doc 9303-10 and Doc 9303-11. After issuance a locked contactless IC cannot be unlocked.

Public Key Infrastructure (*PKI)*

The aim of the PKI scheme, as described, is mainly to enable eMRTD inspecting authorities (receiving States or organizations) to verify the authenticity and integrity of the data stored in the eMRTD. The specifications do not try to prescribe a full implementation of a complicated PKI structure, but rather are intended to provide a way of implementation in which States or organizations are able to make choices in several areas (such as active authentication, anti-skimming and access control, automated border crossing, etc.), thus having the possibility to phase in implementation of additional features without being incompliant with the total framework.

Certificates are used for security purposes, along with a methodology for public key (certificate) circulation to States or organizations, and the PKI is customized for ICAO purposes.

The PKI specifications are described in detail in Doc 9303-12.

6. TEST METHODOLOGIES FOR eMRTDS

ICAO, in cooperation with ISO, has developed test methodologies for qualifying eMRTDs with respect to their conformance to the specifications set out in Doc 9303, parts 9, 10, 11, and 12. These test methodologies are specified in ICAO Technical Reports, being maintained under the coordination of ISO/IEC JTC1 SC17 WG3.

Issuing States and organizations are RECOMMENDED to qualify their eMRTDs, inspection systems and PKI solutions according to the test specifications listed hereunder:

ISO/IEC 18745-2	Specific tests on the contactless interface for eMRTDs
ICAO TR RF & PROTOCOL P3	LDS and Protocol testing
ICAO TR RF & PROTOCOL P4	Tests for inspection systems
ICAO TR RF & PROTOCOL P5	Tests for PKI objects

7. REFERENCES (NORMATIVE)

ICAO TR RF & PROTOCOL P3	RF Protocol and Application Test Standard for eMRTD — Part 3: Tests for Application Protocol and Logical Data Structure
ICAO TR RF & PROTOCOL P4	RF Protocol and Application Test Standard for eMRTD — Part 4: Conformity Test for Inspection Systems
ICAO TR RF & PROTOCOL P5	RF Protocol and Application Test Standard for eMRTD — Part 5: Tests for PKI objects
ISO/IEC 2382-37	Information Technology – Vocabulary – Part 37: Biometrics
ISO/IEC 7816-4	ISO/IEC 7816-4:2013, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange
ISO/IEC 10373-6	ISO/IEC 10373-6:2016 Identification cards — Test methods — Part 6: Proximity cards
ISO/IEC 18745-2	ISO/IEC 18745-2:2016 Information technology — Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test methods for the contactless interface
ISO/IEC 14443-1	ISO/IEC 14443-1:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics
ISO/IEC 14443-2	ISO/IEC 14443-2:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface.

	Note.— Latest revisions of ISO/IEC 14443-2 stipulate limits of EMD as REQUIRED. However eMRTDs issued to the field and in process do not necessarily conform to this new parameter. To maintain backwards compatibility for compliance the EMD limits referenced in ISO/IEC 14443-2 should remain as OPTIONAL for eMRTDs within Doc 9303.
ISO/IEC 14443-3	ISO/IEC 14443-3:2016 (corrected version 2016-09-01), Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision
ISO/IEC 14443-4	ISO/IEC 14443-4:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol
ISO/IEC 19794-4	ISO/IEC 19794-4:2005, Information technology — Biometric data interchange formats — Part 4: Finger image data
ISO/IEC 19794-5	ISO/IEC 19794-5:2005, Information technology — Biometric data interchange formats — Part 5: Face image data
ISO/IEC 19794-6	ISO/IEC 19794-6:2005, Information technology — Biometric data interchange formats — Part 5: Iris image data
ISO/IEC 39794-4	ISO/IEC 39794-4, Information technology — Extensible biometric data interchange formats — Part 4: Finger image data
ISO/IEC 39794-5	ISO/IEC 39794-5, Information technology — Extensible biometric data interchange formats — Part 5: Face image data
ISO/IEC 39794-6	ISO/IEC 39794-6, Information technology — Extensible biometric data interchange formats — Part 6: Iris image data

— — — — — — — —

Appendix to Part 9

PROCESS FOR READING eMRTDS (INFORMATIVE)

A.1 PRECAUTIONS IN eMRTD MANUFACTURE

Issuing States or organizations need to ensure the manufacturing process and the personalization process do not introduce unexpected damage to the IC or to its antenna. For example, excessive heat in lamination or image perforation in the area of the IC or its antenna may damage the IC assembly. Similarly, when the IC is in the front cover, foil blocking on the outside of the cover, after it is assembled, can also damage the IC or the connections to its antenna.

A.2 READING BOTH THE OCR AND THE DATA ON THE IC

It is strongly recommended that a receiving State or organization read both the OCR data and the data stored on the IC. Where an issuing State or organization has locked the IC against eavesdropping, the reading of the OCR is required in order to access the IC data. It is desirable that only one reader be used for both operations, the reader being equipped to read both. If the MRP is opened at the data page and placed on a whole page reader, some MRPs will have the IC situated behind the face of the data page, while others will have the IC in the part of the book that is not in the whole page reader.

A.3 READING GEOMETRIES

States and organizations shall therefore install reading equipment capable of handling MRPs of both geometries, preferably capable of reading both OCR and the IC. Figure 6 shows possible reader configurations, each capable of reading the OCR and the IC. The book is half opened and two antennas ensure that the IC is read irrespective of whether or not it faces the MRZ. Also shown is a less satisfactory configuration in which the eMRTD is placed on an OCR reader or swiped through an OCR reader to read the MRZ and then on a reader for the IC data. This arrangement will be less convenient for immigration staff.

Reading geometries

Reader manufacturers therefore need to consider how to design machine reading solutions that account for the various orientation possibilities and (ideally) are capable of reading the MRZ and the contactless IC simultaneously.

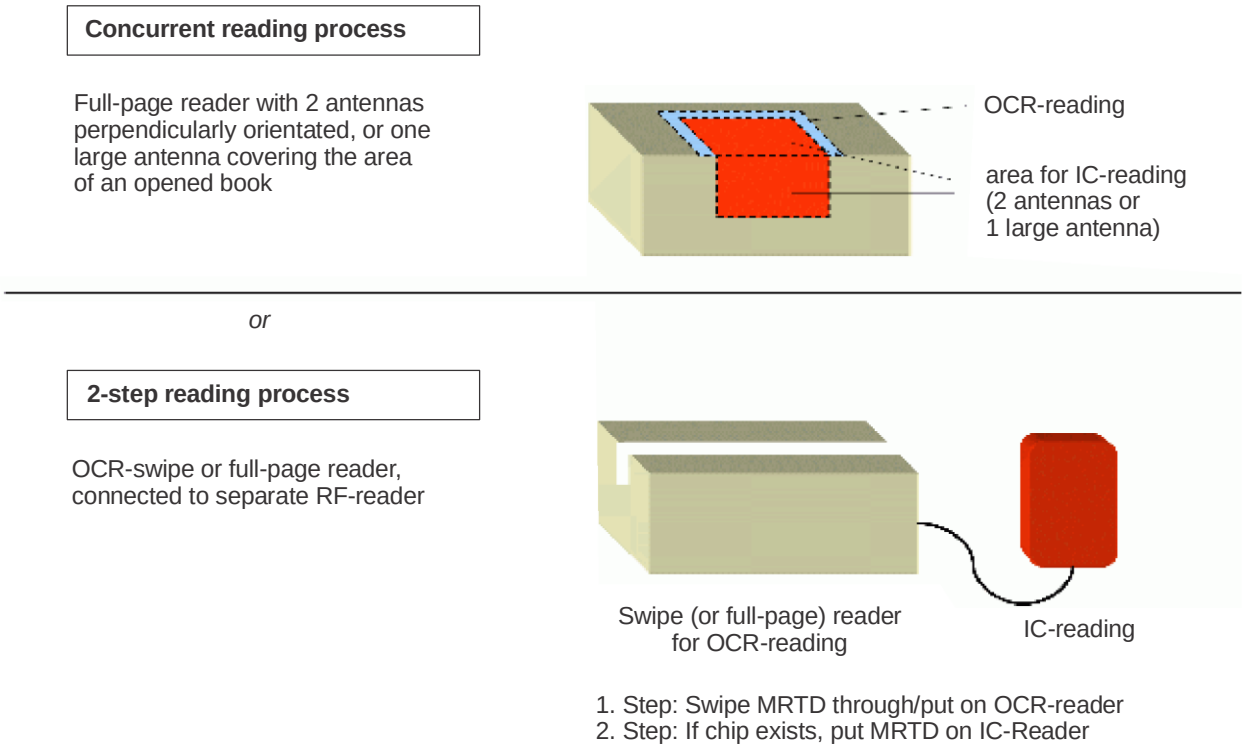


Figure 6. Reading geometries

A.4 READING PROCESSES

Figure 7 shows the processes involved in the reading of an eMRTD prior to and including the biometric verification of the holder.

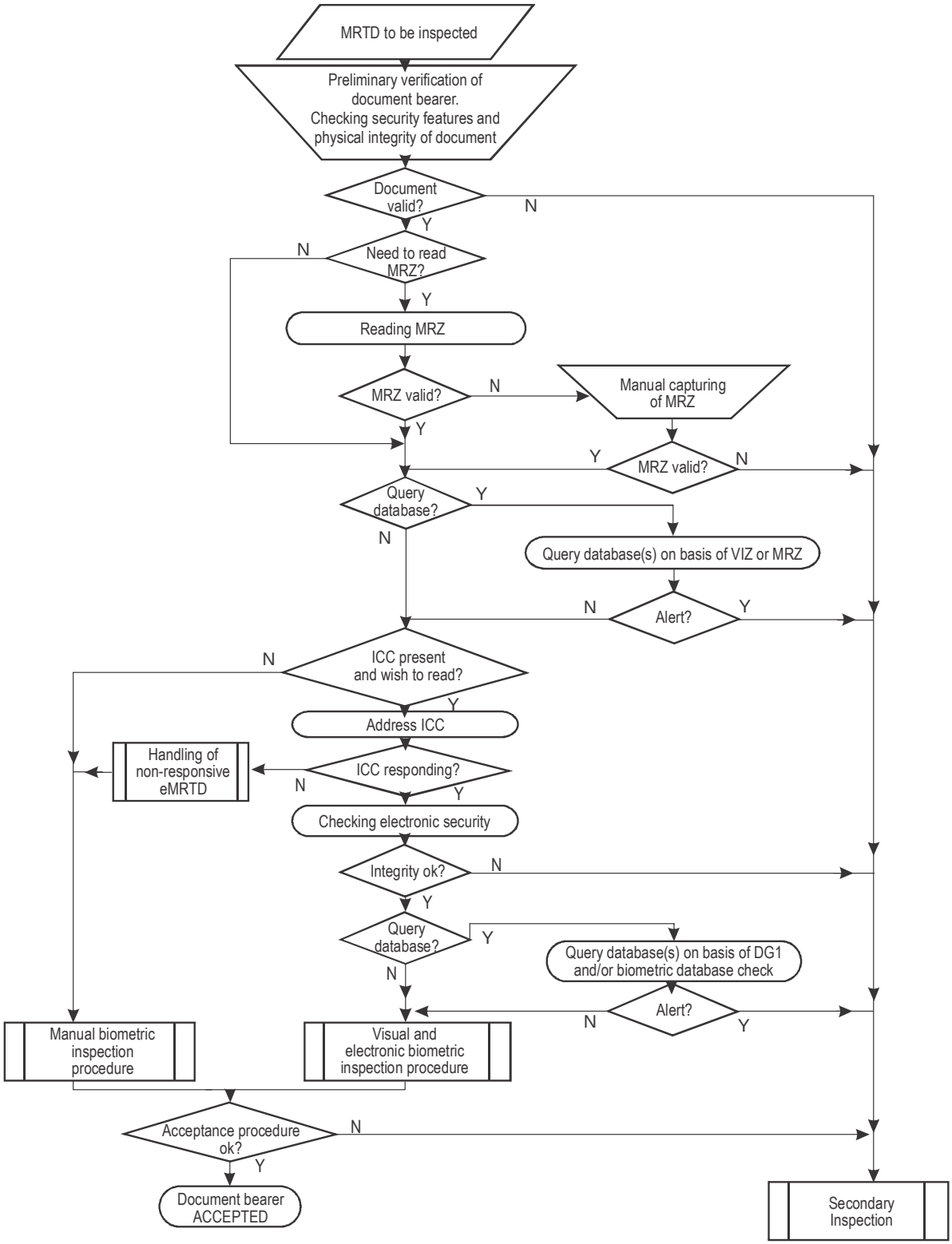


Figure 7. eMRTD reading process

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 202x

Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 10 — *Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*
ISBN 978-92-9249-798-9

DOCUMENT CHANGE RECORD

Doc 9303, Part 10

DATE	NO.	SECTION/PAGES AFFECTED

Table of contents

1 SCOPE

This Part 10 of Doc 9303 defines the Logical Data Structure (LDS) for eMRTDs required for global interoperability and defines the specifications for the organization of data on the contactless IC. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that MUST be followed to achieve global interoperability for electronic reading of the electronic passport.

Doc 9303-10 provides specifications to enable States and integrators to implement a contactless IC into an electronic travel document. This part defines all mandatory and optional data elements, file structures, and application profiles for the contactless IC.

The Eight Edition of Doc 9303 incorporates the specifications for the optional Travel Records, Visa Records, and Additional Biometrics applications (known as LDS2 applications) as an extension of the mandatory eMRTD application (known as LDS1).

Part 10 shall be read in conjunction with:

- Part 1 — *Introduction*;
- Part 3 — *Specifications Common to all MRTDs*;
- Part 4 — *Specifications for Machine Readable Passports (MRP) and other TD3 size MRTDs*;
- Part 5 — *Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)*;
- Part 6 — *Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)*.

and the relevant contactless IC parts:

- Part 9 — *Deployment of Biometric Identification and Electronic Storage of Data in MRTDs;*
- Part 11 — *Security Mechanisms for MRTDs*;
- Part 12 — *Public Key Infrastructure for MRTDs*.

2 STRUCTURE OF Doc 9303-10

Doc 9303 Part 10 is organized into sections to include:

Section 3 Specifications common to both LDS1 and LDS2 applications:

- Common attributes;
- All commands for both LDS1 and LDS2;
- Common Elementary Files (EFs) for both LDS1 and LDS2.

Section 4 Specifications for the LDS1 eMRTD application.

Section 5 Specifications for the LDS2 applications:

- Travel Records;
- Visa Records;
- Additional Biometrics;
- Specifications for LDS2 file access conditions.

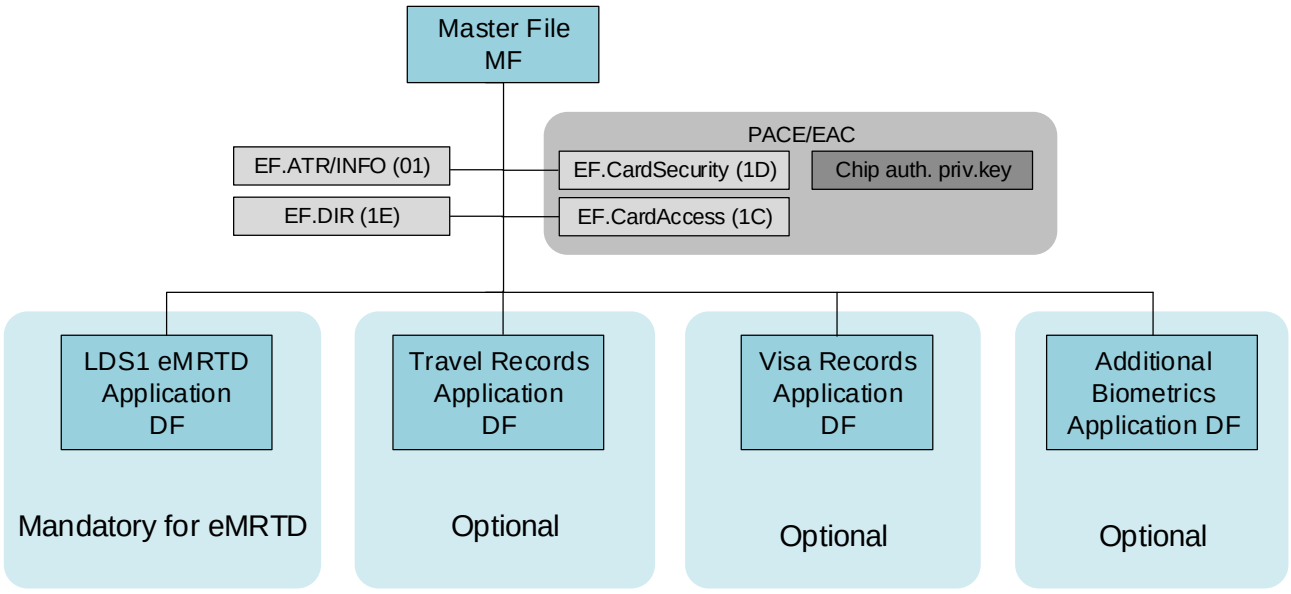


Figure 1: Applications for both LDS1 and LDS2

The eMRTD may support one, several or all of these:

- LDS1 eMRTD application MANDATORY;
- LDS2 Travel Records application OPTIONAL;
- LDS2 Visa Records application OPTIONAL;
- LDS2 Additional Biometrics application OPTIONAL.

3 SPECIFICATIONS COMMON TO LDS1 AND LDS2

3.1 Minimum Requirements for Interoperability

The following SHALL be the minimum requirements for interoperability of proximity contactless IC-based electronic passport:

- [ISO/IEC 14443-1], [ISO/IEC 14443-2], [ISO/IEC 14443-3], [ISO/IEC 14443-4] including all associated amendments, and corrigendums;
- [ISO/IEC 10373-6] test specification compliant including all associated amendments and corrigendum;
- Type A or Type B signal interface;
- Support for a file structure as defined by [ISO/IEC 7816-4] for variable length transparent files;
- Support for one or more applications and appropriate [ISO/IEC 7816-4] commands as specified in Doc 9303.

3.2 Electrical Characteristics

The radio frequency power and signal interface SHALL be as defined in [ISO/IEC14443-2]. A minimum of 424 kilobits per second transmission speed is advised. Use of the EMD features specified in [ISO/IEC 14443-2] is OPTIONAL.

3.3 Physical Characteristics

It is recommended that the size of the coupling antenna area be in accordance with [ISO/IEC 14443-1] Class 1 (ID-1 antenna size) only.

3.4 Transmission Protocol

The eMRTD SHALL support half-duplex transmission protocol defined in [ISO/IEC14443-4]. The eMRTD SHALL support either Type A or Type B transmission protocols, and Initialization, Anticollision and Transmission Protocols according to ISO/IEC 14443.

3.4.1 Request Command and Answer to Request

The contactless IC SHALL respond to Request Command Type A (REQA) or Request Command Type B (REQB) with Answer to Request Type A (ATQA) or Answer to Request Type B (ATQB), as appropriate.

3.4.2 Random vs Fixed Identifier for the Contactless IC

The eMRTD may serve as a “beacon” in which the contactless IC emits a Unique Identifier (UID) for Type A, and PUPI for Type B when initially activated. This might allow identification of the issuing authority. [ISO/IEC 14443] allows the choice of the option whether the eMRTD presents a fixed identifier, assigned uniquely for only that eMRTD, or a random number, which is different at each start of the communication dialogue. Some issuing States prefer to implement a unique number for security reasons or any other reason. Other issuers give greater preference to concerns about data privacy and the possibility to track persons due to fixed IC identifiers.

Choosing the one or the other option does not decrease interoperability since a reader terminal when compliant with ISO/IEC 14443 will understand both methods. The use of random IC identifiers is RECOMMENDED, but States MAY choose to apply unique UIDs for Type A or unique PUPIs for Type B.

3.5 Command Set

All commands, formats, and their status bytes are defined in [ISO/IEC 7816-4] and [ISO/IEC 7816-8] with the exception of the FILE AND MEMORY MANAGEMENT command. The minimum set of commands to be supported by the LDS1 eMRTD MUST be as follows:

SELECT;
READ BINARY.

It is recognized that additional commands will be required to establish the correct security environment and implement the optional security provisions identified in Doc 9303-11**.** Implementation of the mechanisms specified in Doc 9303-11 requires support of the following additional commands:

GET CHALLENGE;
EXTERNAL AUTHENTICATE / MUTUAL AUTHENTICATE;
INTERNAL AUTHENTICATE;
MANAGE SECURITY ENVIRONMENT;
GENERAL AUTHENTICATE.

If optional LDS2 applications are present, the eMRTD SHALL additionally support the following commands:

For the Travel Records Application:

READ RECORD;
APPEND RECORD;
SEARCH RECORD;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

For the Visa Records Application:

READ RECORD;
APPEND RECORD;
SEARCH RECORD;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

For the Additional Biometrics Application:

UPDATE BINARY;
READ RECORD;
APPEND RECORD;
SEARCH RECORD;
ACTIVATE;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

Further details on command protocols can be found in Doc 9303-11.

3.5.1 SELECT

The LDS1 eMRTD supports two structure selection methods that are file identifier and short EF identifier. Readers support at least one of the two methods. The file identifier and Short EF Identifier is MANDATORY for the contactless IC operating system, but OPTIONAL for the reader.

3.5.2 READ BINARY

The support of the READ BINARY command with an odd INS byte by an eMRTD is CONDITIONAL. The eMRTD

SHALL support this command variant if it supports data groups with 32 768 bytes or more.

3.6 Command Formats and Parameter Options (LDS1 and LDS2)

3.6.1 Application DF Selection Using SELECT Command

Applications have to be selected by their DF name indicating the application identifier (AID). After the selection of an application, the file within this application can be accessed.

Note: DF names have to be unique. Therefore selection of an application using the DF name can be done from wherever needed.

3.6.1.1 Selection of Master File

Table 1. SELECT Command for MF Selection

CLA	'00'
INS	'A4'
P1	'00'
P2	'0C'
Lc field	Absent
Data field	Absent
Le field	Absent

SELECT Command Response

Data field	Absent
SW1-SW2	'9000' Normal processing Other values indicate Checking or Execution error

Note:It is RECOMMENDED that the SELECT MF command not be used.

3.6.1.2 Selection of Application DF

An application DF SHALL be selected by using SELECT command with DF name indicating application identifier (AID). The parameters for the APDU command are shown below:

Table 2. SELECT Command with AID for Application DF Selection

CLA	'00'
INS	'A4'
P1	'04'
P2	'0C'
Lc field	Length of the command data field
Data field	DF name (AID)
Le field	Absent

SELECT Command Response

Data field	Absent
SW1-SW2	'9000' Normal processing Other values indicate Checking or Execution error

3.6.2 EF Selection Using SELECT Command

EF is selected by the SELECT command with EF identifier. When the EF is selected, it has to be assured that the application DF storing the EF has previously been selected.

Table 3. SELECT Command with File Identifier for EF Selection

CLA	'00' / '0C'
INS	'A4'
P1	'02'
P2	'0C'
Lc field	'02'
Data field	File Identifier
Le field	Absent

SELECT Command Response

Data field	Absent
SW1-SW2	'9000' Normal processing Other values indicate Checking or Execution error

The eMRTD SHALL support the SELECT command with file identifier as specified in Table 3. The inspection system SHALL support at least one of the following methods:

- The SELECT command with file identifier as specified in Table 3;
- The READ BINARY command with even INS code and short EF identifier as specified in Table 5.

3.6.3 Reading Data from EF (READ BINARY)

There are two methods to read data from the eMRTD: by selecting EF then reading the data of the selected EF, or by reading the data directly using the short EF identifier. Support for short EF identifier is MANDATORY for the eMRTD. It is therefore RECOMMENDED that the inspection system use short EF identifier.

3.6.3.1 Reading Data From Selected EF (Transparent File)

Table 4. READ BINARY Command for Selected EF

CLA	'00' / '0C'
INS	'B0'
P1	Offset
P2	
Lc field	Absent
Data field	Absent
Le field	Present for encoding Ne > 0

READ BINARY Command Response

Data field	Data read
SW1-SW2	'9000' Normal processing Other values indicate Checking or Execution error

3.6.3.2 Reading Data Using EF Identifier (Transparent File)

Table 5. READ BINARY Command with Short EF Identifier

CLA	'00' / '0C'
INS	'B0'
P1	Short EF Identifier
P2	Offset
Lc field	Absent

Data field	Absent
Le field	Present for encoding Ne > 0. Maximum number of bytes expected in the response data field

READ BINARY Command Response

Data field	Data read
SW1-SW2	'9000' Normal processing Other values indicate Checking or Execution error

3.6.4 Extended Lc/Le Support

Depending on the size of the cryptographic objects (e.g. public keys, signatures), APDUs with extended length fields MUST be used to send this data to the eMRTD chip. For details on extended length field, see [ISO/IEC 7816-4].

3.6.4.1 Extended Length and eMRTD Chips

For eMRTD chips, support of extended length field is CONDITIONAL. If the cryptographic algorithms and key sizes selected by the issuing State require the use of extended length field, the eMRTD chips SHALL support extended length field. If the eMRTD chip supports extended length field this MUST be indicated in the ATS or in EF.ATR/INFO as specified in [ISO/IEC 7816-4].

3.6.4.2 Terminals

For terminals, support of extended length field is MANDATORY. A terminal SHOULD examine whether or not support for extended length field is indicated in the eMRTD chip's ATR/ATS or in EF.ATR/INFO before using this option. The terminal MUST NOT use extended length field for APDUs other than the following commands unless the exact input and output buffer sizes of the eMRTD chip are explicitly stated in the ATS or in EF.ATR/INFO:

- MSE:Set KAT;
- GENERAL AUTHENTICATE.

3.6.5 Command Chaining

Command chaining MUST be used for the GENERAL AUTHENTICATE command to link the sequence of commands to the execution of the protocol. Command chaining MUST NOT be used for other purposes unless clearly indicated by the chip. For details on command chaining, see [ISO/IEC 7816-4].

3.6.6 EFs Greater Than 32 767 Bytes

The maximum size of an EF is normally 32 767 bytes, but some contactless ICs support larger files. A different READ BINARY parameter option and command format is required to access the data area when the offset is greater than 32 767. This format of command SHOULD be used after the length of the template has been determined and the need to access the data in the extended data area has been determined. For example, if the data area contains multiple biometric data objects, it may not be necessary to read the entire data area. Once the offset for the data area is greater than 32 767, this command format SHALL be used. The offset is placed in the command field rather than in the parameters P1 and P2.

Table 6. READ BINARY Command Format When Offset is Greater Than 32 767 Bytes

CLA	'00' / '0C'
INS	'B1'
P1	See Table 7
P2	
Lc field	Length of the command data field
Data field	Offset DO'54
Le field	Present for encoding Ne > 0.

	Maximum number of bytes expected in the response data field

READ BINARY Command Response

Data field	Discretionary DO'53'
SW1-SW2	'9000' Normal processing Other values indicate Checking or Execution error

Table 7. P1-P2 Coding of READ BINARY Command with INS=B1

P1								P2								Meaning
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b8**	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Selected EF
0	0	0	0	0	0	0	0	0	0	0	Not all equal					Short EF identifier
Not all zero								X	X	X	X	X	EF identifier			

Both Length and Value fields of BER-TLV data object are variable length and can be encoded in different ways (see [ISO/IEC 7816-4]: "BER-TLV length fields").

For performance reasons, communication between the eMRTD and the terminal SHOULD be kept as short as possible. Therefore, Length field and Value field in the BER-TLV data object SHOULD be as short as possible. This applies not only for Offset data objects in odd INS READ BINARY commands but also for all other BER-TLV data objects exchanged between the eMRTD and the terminal.

Examples for encoded Offset in Data-field:

- Offset: '0001' is encoded as Tag='54' Length='01' Value='01';
- Offset: 'FFFF' is encoded as Tag= '54' Length='02' Value='FFFF'.

The subsequent READ BINARY commands SHALL specify the offset in the Data field. The final READ BINARY command SHOULD request the remaining data area.

With respect to [ISO/IEC 7816-4], there are no constraints specified on the offset value when bit 1 of INS is set to 1 to allow a broader use.

Note 1: In some instances there are eMRTDs where, B1 and the traditional B0 READ Binary commands could not overlap. In other words, B0 only should be used to read the first 32 767 bytes and B1 from 32 K upward. For others there could be a small overlap of 256 bytes around the 32 767 threshold to allow a smoother transition between B0 and B1. For this latter group, B1 could be used right from the beginning of the file, i.e. with an offset starting from 0 to allow the same command to be used to read the full content.

Note 2: The odd INS byte is not to be used by the inspection system if the size of an EF is 32 767 bytes or less.

3.7 Records Handling and Commands (LDS2)

Travel Records, Visa Records and Certificates MUST be stored in EF under the respective applications and having Linear Structure with Records of Variable Size. See Figure 4 and 5.

Records within each EF MUST be referenced by a record number. Each record number MUST be unique and sequential (zero referencing the selected record is out of the scope of this document).

Within each EF supporting a linear structure, the record numbers MUST be sequentially assigned when appending, such as in the order of creation; the first record (number one) is the first created record.

The following [ISO/IEC 7816-4] commands MUST be used for records access:

- APPEND RECORD Appending of Travel Records, Visas, Certificates;
- READ RECORD (S) Reading of one or more Travel Records, Visas, Certificates;
- SEARCH RECORD Searching of one or more Travel Records, Visas, Certificates.

Note: Acronyms used in this sub-section are defined in [ISO/IEC 7816-4].

3.7.1 APPEND RECORD Command

The command initiates the appending of a new record at the end of a linear structure.

Table 8: APPEND RECORD Command

CLA	'0C'
INS	'E2'
P1	'00' (any other value is invalid)
P2	See Table 10
Lc field	Length of the command data field
Data field	Record to be appended
Le field	Absent

Table 9: APPEND RECORD Response

Data field	Absent
SW1-SW2	'9000' Normal processing; '6A84' Not enough memory space in the file; '6700' Wrong length (the record to be appended is longer than the specified maximum length); Other values for indicating Checking or Execution error

Table 10: Coding of P2 in the APPEND RECORD Command

b8	*b7*	*b6*	*b5*	*b4*	*b3*	*b2*	*b1*	*Meaning*
x	*x*	*x*	*x*	*x*	*-*	*-*	*-*	*Short EF identifier*
-	*-*	*-*	*-*	*-*	*0*	*0*	*0*	*Any other value is RFU*

3.7.2 READ RECORD Command

The command returns the full or partial content of one or more addressed record(s) of the selected EF. Depending on the record size and the content of Le field, the response data field contains one of the following:

- the beginning part of the addressed record;
- one (or more) full addressed record(s);
- one (or more) full addressed record(s) followed by the beginning part of the next record.

See [ISO/IEC 7816-4] for details and Appendix H for an example of reading of the travel record.

Figure 2 illustrates the response data field. The comparison of N_r with the TLV structure indicates whether the unique record (read one record) or the last record (read all records) is incomplete, complete or padded.

Table 11: READ RECORD Command

CLA	'0C'	
INS	'B2'	
P1	Record number ('00' references the current record)	
P2	See Table 13	
Lc field	Absent	
Data field	INS = 'B2'	Absent
Le field	Maximum number of bytes to be read encoded as extended length field; Le = '00 00 00' (any other value is out of the scope of the specification)	

Table 12: READ RECORD Response

Data field	Data read
SW1-SW2	'9000' Normal processing; '6A83' (Record not found); Other values for indicating Checking or Execution error

Table 13: Coding of P2 with the READ RECORD Command

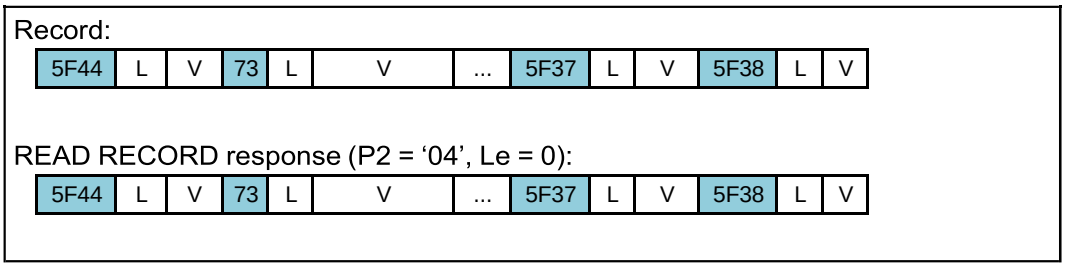
b8	***b7***	***b6***	***b5***	***b4***	***b3***	***b2***	***b1***	***Meaning***
x	*x*	*x*	*x*	*x*	-	-	-	*Short EF identifier*
-	-	-	-	-	*1*	*x*	*x*	***Record number in P1***
-	-	-	-	-	*1*	*0*	*0*	*— Read record P1*
-	-	-	-	-	*1*	*0*	*1*	*— Read all records from P1 up to the last*

Note: Other bits combinations are out of scope of this specification

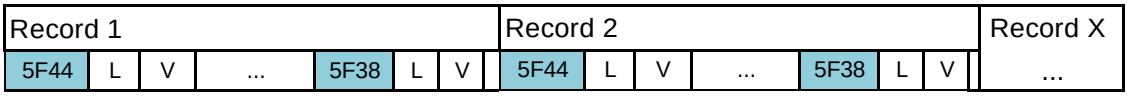
If the Le field contains only bytes set to '00', then the command should read completely either the single requested record, or the requested sequence of records, depending on bits 3, 2 and 1 of P2 and within the limit of maximum supported length for extended Le field.

Note: The READ RECORD command with short length fields is out of the scope of this specification.

Case a — Complete read of one record (the Le field contains only bytes set to '00')



Case b — Read several records up to the file end (the Le field contains only bytes set to '00')



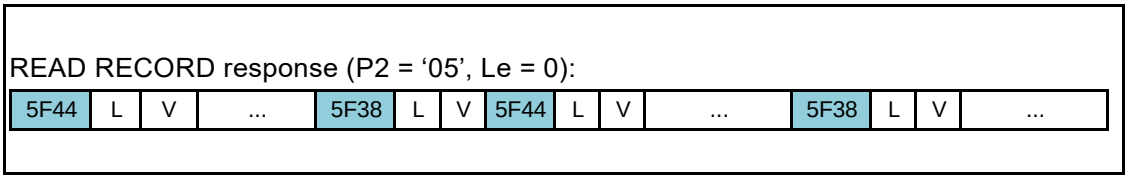


Figure 2: Response Data Fields

3.7.3 SEARCH RECORD Command

The command initiates a search on records stored within the respective EF. The command data field contains Record handling DO’7F76’ defining file reference, search configuration and search string (see Table 17). The response data field returns the Record handling DO’7F76’ containing one or more DO’02’ containing the record number matching the search criteria within the addressed EF.

In an EF supporting records of variable size with linear structure, the search MAY NOT take into account the records with a search window shorter than the search string.

Table 14: SEARCH RECORD Command

CLA	‘0C’
INS	'A2'
P1	'00'
P2	See Table 16
Lc field	Length of command data field
Data field	Record handling DO'7F76' (See Table 17)
Le field	‘00’ (short length) or ’00 00’ (extended length)

Table 15: SEARCH RECORD Response

Data field	Record handling template DO‘7F76‘containing one file reference DO‘51‘ with one or more integer DO‘02‘ containing record number matching the search criteria
SW1-SW2	‘9000’ Normal processing; '6282' Warning: Unsuccessful search Other values for indicating Checking or Execution error

Note: The response data field may be absent if no match is found.

Table 16: Coding of P2 for the SEARCH RECORD Command

b8	***b7***	***b6***	***b5***	***b4***	***b3***	***b2***	***b1***	***Meaning***
1	*1*	*1*	*1*	*1*	*0*	*0*	*0*	*Search record through multiple EFs*
- Any other value is RFU.								

Table 17: Record Handling Template for Enhanced Multiple Record Search

Tag	Value				Notes
'7F76'					Record handling DO
	Tag	**Value**			
	'51'	File identifier or short EF identifier			File reference DO
	'A1'				Search configuration template
		Tag	**Value**		
		'80'	'00' / '30'		Search configuration parameter: - search in record number ascending order - step-width for the search: byte-wise - search termination: '00' - Search all addressed records '30' - Terminate search after first matching
		'B0'			Search window template
			Tag	**Value**	
			'02'	Offset	
			'02'	Number of bytes	
	Tag	**Value**			
	'A3'				Search string template
		Tag	**Value**		
		'B1'			
			Tag	**Value**	
			'81'	Search string	

Note 1: An empty offset DO in the search window template is not supported.

Note 2: If the search window template makes use of the value '00' for the number of bytes, the LDS2 eMRTD chip MUST search all bytes from the offset in the records.

Note 3: The SEARCH RECORD command supports only the DOs specified in Table 17. This implies that the SEARCH RECORD command supports exactly 1 file reference DO in the record handling DO and exactly 1 search string in the search string template. The command MAY ignore additional DOs or answer with an error code if additional DOs are used.

3.8 Transparent Files Handling and Other (LDS2)

The Additional Biometrics transparent EFs are created by the LDS2 eMRTD issuer in Operational Deactivated state (creation mechanism is out of scope of this specification). In Deactivated state the EF can be selected, written, updated and read with appropriate authorizations.

The following [ISO/IEC 7816-4] commands MUST be used for writing and reading Additional Biometrics transparent EF:

- UPDATE BINARY Writing of Additional Biometrics;
- READ BINARY Reading of Additional Biometrics.

The following [ISO/IEC 7816-9] command MUST be used for activating the transparent EF after writing and optional reading and verification are successfully finished:

- ACTIVATE Activating of Additional Biometrics EF.

Note: Acronyms used in this sub-section are defined in [ISO/IEC 7816-4].

In Activated state the EF can be selected and read with appropriate authorizations (related to the Activated state), but can't be written (appended or updated) with any authorization.

The FILE AND MEMORY MANAGEMENT (FMM) command MUST be used before writing to determine if there is enough available memory space in the EF.

The IS MUST use the following writing sequence for the EF.Biometrics:

1) The first UPDATE BINARY (odd INS) command MUST contain the following DOs in the data field:
   - DO'54' containing the offset '00';
   - DO'53' which MAY contain the first block of the data to be stored. This DO MAY be empty ('53 00');and
   - Proprietary DO'C0 indicating the total EF size (memory size to allocate) is optional.

Note1:The LDS2 eMRTD MAY use the EF size information in DO'C0' for the internal memory allocation (e.g. for explicit dynamic memory allocation). If the LDS2 eMRTD doesn't support the EF size information DO (ex., memory has been allocated statically by the issuer, or LDS2 eMRTD supports implicit dynamic EF memory reallocation), then the LDS2 eMRTD MAY ignore the DO'C0, proceed with writing of the first block of the EF and return '9000', or it MAY return the '6A80' (incorrect parameter in the command data field) error.

Note 2: If the LDS2 eMRTD returns any error in response to UPDATE BINARY with the proprietary DO'C0', then the IS MUST send the standard [ISO/IEC 7816-4] UPDATE BINARY (odd INS) command with zero offset DO'54' and DO'53', without the DO'C0'.

2) Subsequent UPDATE BINARY (odd INS, without DO'C0') commands SHOULD use the offset n+1 where n denotes the number of bytes written so far to the EF.Biometrics. I.e. the terminal SHOULD sequentially write the EF data without a gap or overlap between the two consecutive UPDATE BINARY commands.

3) READ BINARY command MAY be used after any UPDATE BINARY command to verify the data written to the EF.

4) The ACTIVATE command MUST finalize EF.Biometrics personalization by permanently disabling writing into the EF.

3.8.1 UPDATE BINARY Command

A contactless IC which supports the Additional Biometrics Application MUST support the UPDATE BINARY command with odd INS byte 'D7' according to the Table 18.
The value of the BER-TLV Offset Data Object in the command data field specifies the offset; the value of

the BER-TLV Discretionary Data Object in the command data field specifies the data to be written; the value of the optional BER-TLV File Size Data Object in the command data field specifies the total EF size. The length fields of these BER-TLV data objects should be encoded as short as possible.

When command data field of UPDATE BINARY command has proprietary DO'C0', the bit 8 of CLA byte of command APDU MUST be set as 1 (CLA='8C').

Table 18: UPDATE BINARY Command with odd INS

CLA	'0C' / '8C'
INS	'D7'
P1	File identifier
P2	'00 00' identifies the current EF
Lc	Length of the command data field
Data field	Offset Data Object (tag '54') || Discretionary Data Object (tag '53') || File Size Data Object (tag 'C0') (optional)
Le	Absent

Table 19: UPDATE BINARY Response

Data field	Absent
SW1-SW2	'9000' Normal processing; '6A84' (Not enough memory space in the file) '6A80' Incorrect parameters in the command data field (ex., DO'C0 not supported) '6982' Security status not satisfied: The EF.Biometrics is in EF Activated state Other values for indicating Checking or Execution error

If the Inspection System does not follow the UPDATE BINARY sequence as specified in Section 3.8 (i.e. the first UPDATE BINARY does not start at offset 0), the LDS2 eMRTD chip MAY terminate the UPDATE BINARY command with an error.

3.8.2 ACTIVATE Command

The ACTIVATE command initiates the transition of the currently selected Additional Biometrics EF from the Deactivated state to the Activated state.

Table 20: ACTIVATE Command

CLA	'0C'
INS	'44'
P1	'00'
P2	'00'
Lc	Absent
Data field	Absent
Le	Absent

Table 21: ACTIVATE Response

Data field	Absent
SW1-SW2	'9000'Normal processing; Other values for indicating Checking or Execution error *Note 1: SW1-SW2='61XX' (normal processing) and SW1-SW2='62XX' or '63XX' (warning processing) are out of the scope of this document.*

After successful execution of this command, the currently selected EF.Biometrics MUST be switched to the Activated state. In case an error occurs (SW different from '9000'), the currently selected EF.Biometrics MUST remain in the Deactivated state.

Immediately after successful execution of this command (SW1-SW2 = '9000'), the effective authorization required to perform an action on the EF.Biometrics MUST be the one corresponding to the Activated state (according to the table 98). The effective authorization corresponding to the Deactivated state MUST NOT raise any access right on the EF.Biometrics anymore.

3.8.3 FILE AND MEMORY MANAGEMENT Command

FILE AND MEMORY MANAGEMENT (FMM) command initiates a query of the used or free memory size for the addressed EF. This command is provided for LDS2 eMRTD as proprietary. This command may be used for checking the available free space for the addressed EF before writing or appending. Also this command may be used for getting the last appended record number for reading. P1 indicates the EF addressing method - current EF or file reference DO'51' can be used. P2 indicates the content of the query. The total number of bytes in the addressed EF with transparent or record structure and the number of existing or remaining records for the addressed record EF are provided. The total number of bytes comprises bytes available in the EF without any structural information. This number excludes any structural information that may be required by the LDS2 eMRTD chip. The assumption for the number of remaining records is that the size of all remaining records is maximum. After a successful FMM command, the referenced EF becomes the current EF.

Table 22: FILE AND MEMORY MANAGEMENT (FMM) Command

CLA	'8C'	
INS	'5F'	
P1	See Table 23	
P2	See Table 24	
Lc	Absent for encoding Nc = 0, present for encoding Nc > 0	
Data field	P1 = '00'	Absent
	P1 = '01'	File reference DO'51' (See [ISO/IEC 7816-4])
Le	'00'	

P1 specifies the EF selection method. P2 contains a bit map specifying which information MUST be included in the response.

Table 23: Coding of P1 in the FFM Command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	Current EF
0	0	0	0	0	0	0	1	File reference DO'51 in the command data field
- Any other value is RFU.								

Table 24: Coding of P2 in the FFM Command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	1	Total number of bytes in the addressed EF
-	-	-	-	-	-	1	-	Number of remaining records in the addressed record EF
-	-	-	-	-	1	-	-	Number of existing records in the addressed record EF
x	x	x	x	x	-	-	-	00000 (any other value is RFU)
- Any other value is RFU.								

Table 25: Coding of DO'51 in the FMM Command Data Field

Tag	Length	Value

'51'	1	Short EF identifier (bits b8 to b4 encode a number from one to thirty; bits b3 to b1 are set to 000)
	2	File identifier

The FMM command response contains a set of DOs representing requested file and memory size information.

Table 26: FMM Command Response

Data field	Absent or control information according to P2. See Table 27.
SW1-SW2	'9000', Checking or Execution error as per [ISO/IEC 7816-4]

Table 27: File and Memory Management

Tag	**Length**	**Value**		
'7F78'	Var.	File and memory management DOs		
		Tag	**Len**	**Value**
		81	Var	Total number of bytes in the addressed EF
		82	Var	Number of remaining records in the addressed record EF
		83	Var	Number of existing records in the addressed record EF

Note 1: The LDS2 eMRTD chip MUST return only the Data objects in the FILE AN MEMORY MANAGEMENT DO that are requested by means of P2.

Note 2: The FMM response data is valid only for the specified EF.FMM response data from different EFs may not be independent, e.g. if different EFs share the available memory. The IS should take this into account if combining FMM response data of different EFs.

Note 3: When secure messaging is applied to the FMM command, SM DO'85' MUST be used for encapsulating encrypted command data.

3.9 File Structure Specifications

Information in an LDS2 eMRTD is stored in a file system defined in [ISO/IEC 7816-4]. The file system is organized hierarchically into dedicated files (DFs) and elementary files (EFs). Dedicated files (DFs) contain EFs or other dedicated files. An optional master file (MF) may be the root of the file system.

Note: The need for a master file is determined by the choice of operating systems, LDS1 or LDS2 applications, and optional access conditions.

3.9.1 Encoding of Data

The following types of coding are permitted for the Data Elements:

A = Alpha character [a..z, A..Z];
N = Numeric character [0..9];
S = Special character ['<'];
B = Binary data;
U = UTF-8 encoded UNICODE characters.

UTF-8 encoding of UNICODE characters:

- For any character equal to or below 127 (hex '7F'), the UTF-8 encoding uses one byte which is the same as the ASCII value;
- For characters equal to or below 2047 (hex '07FF'), the UTF-8 encoding uses two bytes;
  - The first byte has two high bits set and the third bit clear (i.e. hex 'C2' to 'DF');
  - The second byte has the high bit set and the second bit clear (i.e. '80' to 'BF');
- For all characters equal to or greater than 2048 and less that 65535 (hex 'FFFF'), the UTF-8 encoding uses three bytes.

3.10 Application Selection — DF

The eMRTDs SHALL support at least one application as follows:

- The LDS1 eMRTD application is MANDATORY;
  - The LDS1 eMRTD application SHALL consist of data recorded by the Issuing State or organization, Data Groups 1 through to 16 together with the Document Security Object (EF.SOD);
  - The Document Security Object (EF.SOD) within the LDS1 eMRTD application consists of the hash values as defined in Doc 9303-11 and Doc 9303-12 for the Data Groups in use, and is needed to validate the integrity of data created by the issuer and stored in the LDS1 eMRTD Application;
- The LDS1 eMRTD application MAY optionally support the additional LDS2 applications described in Doc 9303 as;
  - Travel Records Application;
  - Visa Records Application;
  - Additional Biometrics Application.

In addition, issuing States or organizations may wish to add other applications. The file structure SHALL accommodate such additional applications, but the specifics of such applications are outside the scope of Doc 9303.

The LDS1 and LDS2 applications SHALL be selected by use of the Application Identification (AID) as a reserved DF name. The Application Identifier (AID) SHALL consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] and a Proprietary Application Identifier Extension (PIX) as specified within this document:

The context of LDS1 eMRTD application uses two different tag allocation schemes for application class tag, such as defined in Doc9303-10 (LDS tag) and [ISO/IEC 7816-6] (Interindustry tag):

- EF.ATR/INFO and EF.DIR use interindustry tag allocation scheme;
- DFs with their containing EFs use LDS tag allocation scheme.

Interindustry tags specified in this document are used in LDS context, so coexistent tag allocation scheme is not required.

3.11 Common Elementary Files (EFs)

The following common EFs for LDS1 and LDS2 application MAY be existed under the MF;

- EF.ATR/INFO;
- EF.DIR;
- EF.CardAccess;
- EF.CardSecurity.

3.11.1 EF.ATR/INFO (CONDITIONAL)

EF.ATR/INFO is a transparent EF contained in the master file and is conditionally REQUIRED if the optional LDS2 application is present. This EF is optional if only LDS1 application is present. The short EF identifier at MF level is '01'.

Table 28: EF.ATR/INFO

File Name	EF.ATR/INFO
File ID	'2F01'
Short EF Identifier	'01'
Select Access	ALWAYS
Read Access	ALWAYS
Write/Update/Erase Access	NEVER
File structure	Transparent
Size	Variable

The contents of the EF.ATR/INFO can be retrieved by using a SELECT command followed by READ BINARY command. The READ BINARY command response data field contains the content of the EF.ATR/INFO.

Table 29: Data Elements of EF.ATR/INFO for LDS2

<table>
<tr><th>Tag</th><th>Length</th><th colspan="4">Value</th><th>Notes</th></tr>
<tr><td rowspan="5">'47'</td><td rowspan="5">'03'</td><td colspan="5">Card capabilities</td></tr>
<tr><td colspan="4">byte 1 - first software function</td><td>b8=1: DF selection by full DF name
b7 to b4 and b1 are out of scope of Doc 9303
b3=1: short EF identifier supported
b2=1: record number supported</td></tr>
<tr><td colspan="4">byte 2 - second software function</td><td>b8, b7, b6 and b5 are out of scope of Doc 9303
b4 to b1=0001: one byte data unit size</td></tr>
<tr><td colspan="4">byte 3 - third software function</td><td>b8=1: command chaining supported
b7=1: Extended Lc and Le fields supported
b6=1: Extended length information in EF.ATR/INFO
b5 to b1 are out of scope of Doc 9303</td></tr>
<tr><td rowspan="4">'7F66'</td><td rowspan="4">Var</td><td colspan="5">Extended length information</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">Value</td><td>Notes</td></tr>
<tr><td>'02'</td><td>Var</td><td colspan="2">Positive integer - the maximum number of bytes in the command data field</td><td>MUST be at least 1000 (decimal) for LDS2</td></tr>
<tr><td>'02'</td><td>Var</td><td colspan="2">Positive integer - the maximum number of bytes expected in the response APDU</td><td>MUST be at least 1000 (decimal) for LDS2</td></tr>
</table>

Note 1: Further data objects MAY be present in EF.ATR/INFO.
Note 2: EF.ATR/INFO uses interindustry tag allocation scheme as defined in [ISO/IEC 7816-4].

3.11.2 EF.DIR (CONDITIONAL)

EF.DIR is a transparent EF contained in the master file defined by [ISO/IEC 7816-4]. EF.DIR is conditionally REQUIRED if any optional LDS2 applications are present. If any optional LDS2 applications are present EF.DIR MUST be included in SecurityInfos present in EF.CardSecurity. A full description of SecurityInfo for EF.DIR can be found in Doc 9303-11.

The short EF identifier at MF level is ’1E'.

Table 30: EF.DIR

File Name	EF.DIR
File ID	’2F00’
Short EF Identifier	’1E'
Select Access	ALWAYS
Read Access	ALWAYS
Write/Update/Erase Access	NEVER
File structure	Transparent
Size	Variable

EF.DIR is RECOMMENDED to be present in the MF. EF.DIR MUST be present if more than the mandatory LDS1 application is present and indicate a list of applications supported by the eMRTD. It MUST contain a set of application templates containing application identifier DO in any order.

Table 31: EF.DIR Format

Tag	L	Value			Description
'61'	'09'				LDS1 eMRTD Application Template
		Tag	**L**	**Value**	LDS1 eMRTD Application International AID: 'A0 00 00 02 47 10 01'
		'4F'	'07'	'A0 00 00 02 47 10 01'	
'61'	'09'				Travel Records Application Template
		Tag	**L**	**Value**	Travel Records International AID: 'A0 00 00 02 47 20 01'
		'4F'	'07'	'A0 00 00 02 47 20 01'	
'61'	'09'				Visa Records Application Template
		Tag	**L**	**Value**	Visa Records International AID: 'A0 00 00 02 47 20 02'
		'4F'	'07'	'A0 00 00 02 47 20 02'	
'61'	'09'				Additional Biometrics Application Template
		Tag	**L**	**Value**	Additional Biometrics International AID: 'A0 00 00 02 47 20 03'
		'4F'	'07'	'A0 00 00 02 47 20 03'	

Note: EF.DIR uses standard tag allocation scheme as defined in [ISO/IEC 7816-4].

3.11.3 EF.CardAccess (CONDITIONAL)

EF.CardAccess is a transparent EF contained in the master file and is conditionally REQUIRED if the optional PACE access control as defined in Doc 9303-11 is invoked. A full description of SecurityInfos for PACE can be found in Doc 9303-11.

The short EF identifier at MF level is '1C'.

Table 32: EF.CardAccess

File Name	EF.CardAccess
File ID	'011C'
Short EF Identifier	'1C'
Select Access	ALWAYS
Read Access	ALWAYS
Write/Update/Erase Access	NEVER
File structure	Transparent
Size	Variable

The file CardAccess contained in the master file is REQUIRED if PACE is supported by the eMRTD chip and SHALL contain the following SecurityInfos that are required for PACE:

- `PACEInfo`;
- `PACEDomainParameterInfo`.

Table 33. EF.CardAccess Storage on the IC

File Name	EF.CardAccess
File ID	'011C'
Short EF ID	'1C'
Read Access	ALWAYS
Write Access	NEVER
Size	Variable
Content	DER encoded SecurityInfos . See Doc 9303-11.

3.11.4 EF.CardSecurity (CONDITIONAL)

EF.CardSecurity is a transparent EF contained in the master file and is conditionally REQUIRED if the optional PACE with Chip Authentication Mapping as defined in Doc 9303-11 is invoked. A full description of `SecurityInfos` for PACE with Chip Authentication Mapping can be found in Doc 9303-11. The short EF identifier at MF level is '1D'.

EF.CardSecurity contained in the MF is REQUIRED if:

- PACE with Chip Authentication Mapping is supported by the IC;
- Terminal Authentication in the MF is supported by the IC; or
- Chip Authentication in the MF is supported by the IC.

and MUST contain:

- ChipAuthenticationInfo as required by Chip Authentication;
- ChipAuthenticationPublicKeyInfo as required by PACE-CAM/Chip Authentication;
- TerminalAuthenticationInfo as required by Terminal Authentication;
- the SecurityInfos contained in EF.CardAccess.

The file EF.CardSecurity contained in the master file is REQUIRED if PACE with Chip Authentication Mapping is supported by the eMRTD chip and SHALL contain the following `SecurityInfos`:

- ChipAuthenticationPublicKeyInfo as required for PACE-CAM;
- The `SecurityInfos` contained in CardAccess.

Table 34. EF.CardSecurity Storage on the IC

File Name	EF.CardSecurity
File ID	'011D'
Short EF ID	'1D'
Read Access	PACE
Write Access	NEVER
Size	Variable

The file CardSecurity SHALL be implemented as SignedData according to [RFC 3369] with content type id-SecurityObject within the field encapContentInfo. The Security Objects SHALL be signed by the Document Signer. The Document Signer Certificate MUST be included in SignedData. The following Object Identifier SHALL be used to identify the content type:

```
bsi-de OBJECT IDENTIFIER ::= {
 itu-t(0) identified-organization(4) etsi(0)
 reserved(127) etsi-identified-organization(0) 7
}
id-SecurityObject OBJECT IDENTIFIER ::= {
 bsi-de applications(3) eID(2) 1
}
```

The data structure SignedData is defined as follows:

```
SignedData ::= SEQUENCE{
 version CMSVersion,
 digestAlgorithms DigestAlgorithmIdentifiers,
 encapContentInfo EncapsulatedContentInfo,
 certificates [0] IMPLICIT CertificateSet OPTIONAL,
 crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
 signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

EncapsulatedContentInfo ::= SEQUENCE {
 eContentType ContentType,
 eContent [0] EXPLICIT OCTET STRING OPTIONAL
}

ContentType ::= OBJECT IDENTIFIER

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
 version CMSVersion,
 sid SignerIdentifier,
 digestAlgorithm DigestAlgorithmIdentifier,
 signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
 signatureAlgoritm SignatureAlgorithmIdentifier,
 signature SignatureValue,
 unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}

SignerIdentifier ::= CHOICE {
 issuerAndSerialNumber IssuerAndSerialNumber,
 subjectKeyIdentifier [0] SubjectKeyIdentifier
}

SignatureValue ::= OCTET STRING
```

4 LDS1 eMRTD APPLICATION (MANDATORY)

The LDS1 eMRTD structure provides space to store and digitally sign mandatory and optional data elements that can be used to link the holder to the document. The information stored in the LDS1 eMRTD portion of the ePassport becomes static at the time of issuance, and cannot be modified in any possible way. This feature is necessary to ensure that personal information is protected, and that document tampering may be more easily detected. While the LDS1 version of eMRTD includes optional data fields that could be used to expand the use of the ePassport (i.e. additional biometrics, automated border clearance, etc...), the requirement of write protecting the LDS1 eMRTD chip application at the time of issuance is MANDATORY.

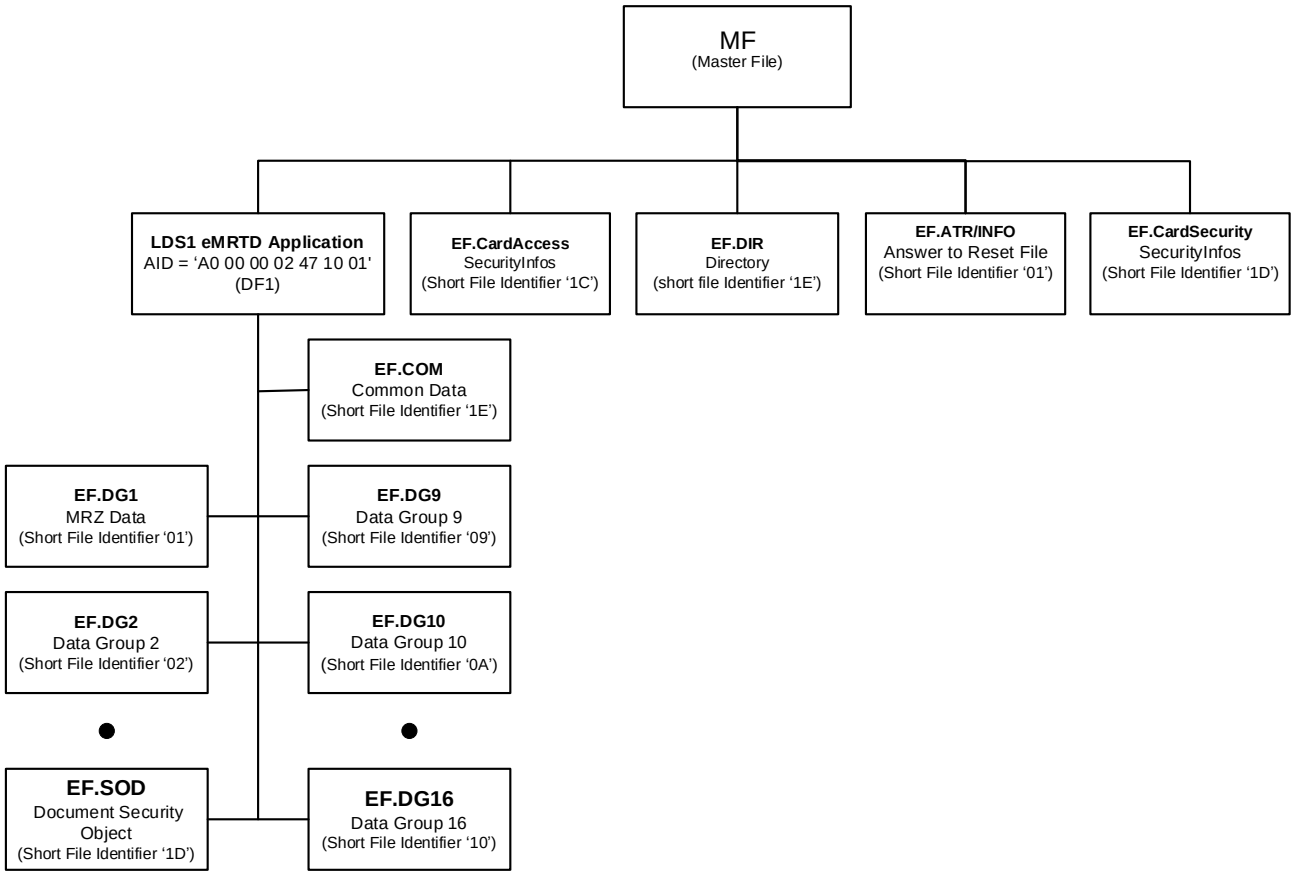


Figure 3: LDS1 eMRTD File Structure Summary

4.1 Application Selection — DF

The LDS1 eMRTD application SHALL be selected by use of the Application Identification (AID) as a reserved DF name. The AID SHALL consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] and a Proprietary Application Identifier Extension (PIX) as specified within this document:

- The Registered Application Identifier is 'A000000247';
- The issuer stored data application SHALL use PIX = '1001';
- The full AID of the LDS1 eMRTD application is 'A0 00 00 02 47 10 01'.

The IC MUST reject the selection of an application if the extension for this application is absent.

4.2 Random Ordering Scheme

The Random Ordering Scheme allows Data Groups and Data Elements to be recorded following a random ordering which is consistent with the ability of the optional capacity expansion technology to allow direct retrieval of specific Data Elements even if they are recorded out of order. Variable length Data Elements are encoded as TLV data objects specified in ASN.1.

4.3 Random Access File Representation

The Random Access File Representation has been defined with the following considerations and assumptions.

Support a wide variety of implementations. The LDS includes a wide variety of optional Data Elements. These Data Elements are included to facilitate LDS1 eMRTD authentication, rightful holder authentication, and to expedite processing at document/person points.

The data structure must support:

- a limited or extensive set of Data Elements;
- multiple occurrences of specific Data Elements;
- continuing evolution of specific implementations.
- Support at least one application data set;
- Allow for other national specific applications;
- Support optional Active Authentication of the document using a stored asymmetrical key pair;
- Support rapid access of selected Data Elements to facilitate rapid document processing:
- immediate access to necessary Data Elements;
- direct access to data templates, and biometric data.

4.4 Grouping of Data Elements

Groupings of Data Elements added by issuing States or approved receiving organizations may or may not be present in an LDS. More than one recording of grouped Data Elements added by receiving States or approved receiving organizations can be present in the LDS.

The ability for a receiving State or approved receiving organization to add data to the LDS is not supported in this edition of Doc 9303.

The LDS is considered to be a single cohesive entity containing the number of groupings of Data Elements recorded in the optional capacity expansion technology at the time of machine reading.

The LDS has been designed with sufficient flexibility that it can be applied to all types of eMRTDs. Within the figures and tables which follow, some data items are only applicable to machine readable visas and to machine readable passports or require a different presentation in relation to these documents.

Within the LDS, logical groupings of related Data Elements have been established. These logical groupings are referred to as Data Groups.

4.5 Requirements of the Logical Data Structure

The contactless IC capacity expansion technology contained in an LDS1 eMRTD selected by an issuing State or organization must allow data to be accessible by receiving States.

ICAO has determined that the predefined, standardized Logical Data Structure (LDS) SHALL meet a number of mandatory requirements:

- ensure efficient and optimum facilitation of the rightful holder;
- ensure protection of details recorded in the optional capacity expansion technology;
- allow global interoperability of capacity expanded data based on the use of a single LDS common to all eMRTDs;

- address the diverse optional capacity expansion needs of issuing States and organizations;
- provide expansion capacity as user needs and available technology evolve;
- support a variety of data protection options;
- utilize existing international specifications to the maximum extent possible, in particular the emerging international specifications for globally interoperable biometrics.

4.5.1 Security

Only the issuing State or organization SHALL have write access to these Data Groups. Therefore, there are no interchange requirements and the methods to achieve write protection are not part of this specification. Once the chip has been locked (after personalization and before issuance) no LDS1 Application data can be written, modified, or deleted to/at/from the chip. After issuance a locked chip cannot be unlocked.

4.5.2 Authenticity and Integrity of Data

To allow confirmation of the authenticity and integrity of recorded details, an authenticity/integrity object is included. Each Data Group MUST be represented in this authenticity/integrity object, which is recorded within a separate EF (EF.SOD). Using the Common Biometric Exchange File Format (CBEFF) structure utilized for Encoded Identification Feature Data Groups 2-4 and optional "additional biometric security" features defined in Doc 9303-12, identity confirmation details (e.g. biometric templates) MAY also be individually protected at the discretion of the issuing State or organization.

4.5.3 Ordering of LDS

The Random Ordering Scheme only SHALL be used for international interoperability.

4.5.4 Data Storage Capacity of the Contactless IC

The data storage capacity of the contactless IC is at the discretion of the issuing State but SHALL be a minimum of 32 kB. This minimum capacity is necessary to store the mandatory stored facial image the MRZ data, and the necessary elements for securing the data. The storage of additional facial, fingerprint and/or iris images may require a significant increase in data storage capacity. There is no maximum contactless IC data capacity specified.

In the event that a State's PKI infrastructure is not available to sign LDS1 eMRTD data as part of personalization, and the issuance of the document(s) cannot be delayed, it is RECOMMENDED that the LDS1 eMRTD contactless IC be left blank and be locked. The LDS1 eMRTD SHOULD contain an appropriate endorsement on this. This is expected to be an exceptional circumstance.

4.5.5 Storage of Other Data

A State MAY use the storage capacity of the contactless IC in an eMRTD to expand the machine readable data capacity of the LDS1 eMRTD beyond that defined for global interoperability. This can be for such purposes as providing machine readable access to identity document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

4.5.6 International Standard for Encoding Biometrics

ISO/IEC 39794 succeeded [ISO/IEC 19794:2005] as international standard for encoding biometrics. The following transition time table has been defined:

- Passport reader equipment MUST be able to handle ISO/IEC 39794 data by 2025-01-01 after a five years preparation period starting 2020-01-01;
- Between 2025 and 2030, passport issuers can use the data formats specified in ISO/IEC 19794-X:2005 or in ISO7IEC 39794-X during a five years transition period. During this transition period, interoperability and conformity testing will be essential;
- From 2030-01-01 on, passport issuers MUST use ISO/IEC 39794-X for encoding biometric data.

ISO/IEC 49794 provides guidance on the transition from [ISO/IEC 19794:2005] to ISO/IEC 39794.

4.6 LDS1 eMRTD Elementary Files (EFs)

4.7 Header and Data Group Presence Information EF.COM (MANDATORY)

EF.COM is located in the LDS1 eMRTD application (Short File Identifier = '1E') and contains LDS version information, Unicode version information and a list of the Data Groups that are present for the application. The LDS1 eMRTD application MUST have only one file EF.COM that contains the common information for the application.

The Data Elements that may occur in this template are as follows:

Table 35: EF.COM Normative Tags

Tag	**L**	**Value**		
60	Var	application level information		
		Tag	**L**	**Value**
		5F01	04	LDS Version number with format aabb, where aa defines the version of the LDS and bb defines the update level.
		5F36	06	Unicode Version number with format aabbcc, where aa defines the major version, bb defines the minor version and cc defines the release level.
		5C	Var	Tag list. List of all Data Groups present.

A Header and Data Group Presence Map SHALL be included. The header SHALL contain the following information which enables a receiving State or approved receiving organization to locate and decode the various Data Groups and Data Elements contained within the block of data recorded by the issuing State or organization.

It is RECOMMENDED that inspection systems that rely on the EF.COM be modified to use the SOD described in the LDS version 1.8 as soon as possible.

4.7.1 LDS version number

The LDS version number defines the format version of the LDS. The exact format to be used for storing this value will be defined in Section 4 of this document. Standardized format for an LDS Version Number is "aabb", where:

- "aa" = number (01-99) identifying the major version of the LDS (i.e. significant additions to the LDS);
- "bb" = number (01-99) identifying the minor version of the LDS.

4.7.2 UNICODE version number

The Unicode version number identifies the coding method used when recording alpha, numeric and special characters, including national characters. The exact format to be used for storing this value will be defined in Section 4.10 of this document. The standardized format for a Unicode version number is "aabbcc", where:

- "aa" = number identifying the major version of the Unicode specification (i.e. significant additions to the specification, published as a book);

- "bb" = number identifying the minor version of the Unicode specification (i.e. character additions or more significant normative changes, published as a technical report); and

- "cc" = number identifying the update version of the Unicode specification (i.e. any other changes to normative or important informative portions of the specification that could change programme behaviour. These changes are reflected in new Unicode character database files and an update page). For historical reasons, the numbering within each of the fields (i.e. a, b, c) is not necessarily consecutive.

The Universal Character Set (UCS) MUST comply with [ISO/IEC 10646].

4.8 Document Security Object EF.SOD (MANDATORY)

In addition to the LDS Data Groups, the contactless IC also contains a Document Security Object stored in EF.SOD. This object is digitally signed by the issuing State and contains hash values of the LDS contents.

Table 36: EF.SOD Tags

Tag	L	Value
77	Var	Document Security Object

There are two versions of the Document Security Object EF.SOD which have been deployed. There is the legacy EF.SOD V0 which can be found in Annex D and the RECOMMENDED EF.SOD V1 in this section. Only one EF.SOD is REQUIRED and allowed.

4.8.1 Document Security Object EF.SOD V1 LDS v1.8)

The Document Security Object V1 for the LDS v1.8 has been extended with a signed attribute, containing the LDS and Unicode version information:

```
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF DataGroupHash,
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1
}

LDSVersionInfo ::= SEQUENCE {
   ldsVersion PrintableString,
   unicodeVersion PrintableString
}
```

4.8.2 SignedData Type for SOD V1

The Document Security Object is implemented as a SignedData Type, as specified in [RFC 3369], Cryptographic Message Syntax (CMS), August 2002. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

Note 1: m REQUIRED — the field SHALL be present.
Note 2: x do not use — the field SHOULD NOT be populated.
Note 3: o optional — the field MAY be present.
Note 4: c choice — the field content is a choice from alternatives.

Table 37: Signed Data Type for SO_D V1

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	m	States are REQUIRED to include the Document Signer Certificate (C_{DS}) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States provide only 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

4.8.3 ASN.1 Profile LDS Document Security Object for SOD V1

```
LDSSecurityObjectV1 { joint-iso-itu-t(2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

-- Imports from RFC 3280 [PROFILE]
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) };

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0), v1(1)
-- If LDSSecurityObjectVersion is v1, ldsVersionInfo MUST be present
}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash,
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1
}

DataGroupHash ::= SEQUENCE {
   dataGroupNumber DataGroupNumber,
   dataGroupHashValue OCTET STRING }

DataGroupNumber ::= INTEGER {
   dataGroup1              (1),
   dataGroup2              (2),
   dataGroup3              (3),
```

```
   dataGroup4              (4),
   dataGroup5              (5),
   dataGroup6              (6),
   dataGroup7              (7),
   dataGroup8              (8),
   dataGroup9              (9),
   dataGroup10            (10),
   dataGroup11            (11),
   dataGroup12            (12),
   dataGroup13            (13),
   dataGroup14            (14),
   dataGroup15            (15),
   dataGroup16            (16)}

LDSVersionInfo ::= SEQUENCE {
   ldsVersion PrintableString
   unicodeVersion PrintableString }
END
```

Note 1: The field `dataGroupHashValue` *contains the calculated hash over the complete contents of the Data Group EF, specified by* `dataGroupNumber`*.*

Note 2: `DigestAlgorithmIdentifiers` *MUST omit "*`NULL`*" parameters, while the* `SignatureAlgorithmIdentifier` *(as defined in RFC 3447) MUST include* `NULL` *as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Inspection system MUST accept the field* `DigestAlgorithmIdentifiers` *with both conditions, i.e. absent parameters and* `NULL` *parameters.*
.

4.9 Data Elements Forming Data Groups 1 Through 16

Data Groups 1 (DG1) through 16 (DG16) individually consist of a number of mandatory, optional, and conditional Data Elements. The specified order of Data Elements within the Data Group SHALL be followed. Each Data Group SHALL be stored in one transparent EF. Addressing EFs SHALL be by Short EF Identifier as shown in Table 38. The EFs SHALL have file names for these files that SHALL be according to the number n, EF.DGn, where n is the Data Group number.

Table 38: Mandatory and Optional Data Elements That Combine to Form the Structure of Data Groups 1 (DG1) Through 16 (DG16)

Data Group	EF Name	Short EF Identifier	EF Identifier	Tag
Common	EF.COM	1E	01 1E	60
DG1	EF.DG1	01	01 01	61
DG2	EF.DG2	02	01 02	75
DG3	EF.DG3	03	01 03	63
DG4	EF.DG4	04	01 04	76
DG5	EF.DG5	05	01 05	65
DG6	EF.DG6	06	01 06	66
DG7	EF.DG7	07	01 07	67
DG8	EF.DG8	08	01 08	68
DG9	EF.DG9	09	01 09	69
DG10	EF.DG10	0A	01 0A	6A
DG11	EF.DG11	0B	01 0B	6B
DG12	EF.DG12	0C	01 0C	6C
DG13	EF.DG13	0D	01 0D	6D
DG14	EF.DG14	0E	01 0E	6E
DG15	EF.DG15	0F	01 0F	6F
DG16	EF.DG16	10	01 10	70
Document Security Object	EF.SOD	1D	01 1D	77
Common	EF.CARDACCESS	1C	01 1C	
Common	EF.ATR/INFO	01	2F 01	
Common	EF.CardSecurity	1D	01 1D	

4.10 DATA GROUP 1 — Machine Readable Zone Information (MANDATORY)

The Data Elements of Data Group 1 (DG1) are intended to reflect the entire contents of the MRZ whether it contains actual data or filler characters. Details on the implementation of the MRZ are dependent on the type of LDS1 eMRTD (TD1,TD2 or TD3 formats).

This Data Element contains the REQUIRED machine readable zone (MRZ) information for the document in template ’61’. The template contains one data object, the MRZ in data object ’5F1F’. The MRZ data object is a composite Data Element, identical to the OCR-B MRZ information printed on the document.

Table 39:Data Group 1 Tags

Tag	L	Value		
61	Var			
		Tag	**L**	**Value**
		5F1F	Var	The MRZ data object as a composite Data Element. (REQUIRED) (The Data Element contains all mandatory fields from Document Type through to Composite check digit.)

4.10.1 DATA GROUP 1 – EF.DG1 Data Elements for TD1 Size LDS1 eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 are intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-5. Data Elements and their format within each Data Group area for TD1 SHALL be as in the following table:

Note: A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character [‘<’], F = fixed-length field.

Table 40: Data Elements for TD1 Format

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Document number (Nine most significant characters)	9	F	A,N,S
04	M	Check digit — Document number or filler character (<) indicating document number exceeds nine characters	1	F	N,S
05	M	Optional data and/or in the case of a Document Number exceeding 9 characters, least significant characters of document number plus document number check digit plus filler character	15	F	A,N,S
06	M	Date of birth	6	F	N,S

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
07	M	Check digit — Date of birth	1	F	N
08	M	Sex	1	F	A,S
09	M	Date of Expiry	6	F	N
10	M	Check digit — Date of expiry	1	F	N
11	M	Nationality	3	F	A,S
12	M	Optional data	11	F	A,N,S
13	M	Composite check digit	1	F	N
14	M	Name of holder	30	F	A,N,S

4.10.2 DATA GROUP 1 — EF.DG1 Data Elements for TD2 Size eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 are intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-6. Data Elements and their format within each Data Group area for TD2 SHALL be as in the following table:

Note: A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 41: Data Elements for TD2 Format

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	31	F	A,N,S
04	M	Document number (Nine principal characters)	9	F	A,N,S
05	M	Check digit	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
11	M	Check digit	1	F	N
12	M	Optional data plus filler character	7	F	A,N,S
13	M	Composite Check Digit - MRZ line 2	1	F	N

4.10.3 DATA GROUP 1 — EF.DG1 Data Elements for TD3 Size LDS1 eMRTD

This section describes the Data Elements that may be present in Data Group 1 (DG1). Storage, ordering and coding requirements of Data Group 1 are intended to be exactly the same as found in the printed MRZ and described in Doc 9303-3 and Doc 9303-4. Data Elements and their format within each Data Group area for TD3 SHALL be as in the following table:

Note: A = Alpha character [A..Z], N = Numeric character [0..9], S = Special character ['<'], F = fixed-length field.

Table 42: Data Elements for TD3 Format

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding
01	M	Document code	2	F	A,S
02	M	Issuing State or organization	3	F	A,S
03	M	Name of holder	39	F	A,S
04	M	Document number	9	F	A,N,S
05	M	Check digit — Document number	1	F	N,S
06	M	Nationality	3	F	A,S
07	M	Date of birth	6	F	N,S
08	M	Check digit — Date of birth	1	F	N
09	M	Sex	1	F	A,S
10	M	Date of expiry	6	F	N
11	M	Check digit — Date of expiry or valid until date	1	F	N
12	M	Optional data	14	F	A,N,S
13	M	Check digit	1	F	N
14	M	Composite check digit	1	F	N

4.11 DATA GROUP 2 — Encoded Identification Features — Face (MANDATORY)

Data Group 2 (DG2) represents the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents, which SHALL be an image of the face of the holder as an input to a face recognition system. If there is more than one recording, the most recent internationally interoperable encoding SHALL be the first entry.

Table 43: Data Group 2 Tags

Tag	L	Value
75	Var	See Biometric encoding of EF.DG2

4.11.1 Biometric encoding of EF

DG2 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and is in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11] is always to be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1.

Each nested template has the following structure:

Table 44: Data Group 2 — Biometric Encoding Tags

Tag	L	Value				
7F61	Var	Biometric Information Template Group Template				
		Tag	**L**	**Value**		
		02	01	Integer — Number of instances of this type of biometric		
		7F60	Var	1st Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version 0101 (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype Optional for DG2
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)

Tag	L	Value				
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

The default OID of CBEFF is used. The OID data object (Tag ’06’) just under Biometric Information Template (BIT, Tag ’7F60’) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the Tag allocation authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-5].

Note: ISO/IEC 39794 will succeed ISO/IEC 19794:2005 as international standard for encoding biometrics. See Part 10 Section 4.5.6

4.11.2 DATA GROUP 2 — EF.DG2 Data Elements

This section describes the Data Elements that may be present in Data Group 2 (DG2): Data Elements and their format within each Data Group area SHALL be as in the following tables:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character [‘<’], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 45: Data Elements for DG2

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M	Number of face biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the face.
02	M	Header		Var	A,N	Data Element may recur as defined by Data element 01.
03	M	Face biometric data encoding(s)		Var	B	Data Element may recur as defined by Data element 01.

4.12 DATA GROUP 3 — Additional Identification Feature — Finger(s) (OPTIONAL)

ICAO recognizes that Member States may elect to use fingerprint recognition as additional biometric technologies in support of machine assisted identity confirmation, which SHALL be encoded as Data Group 3 (DG3).

Table 46: Data Group 3 Tags

Tag	L	Value
63	Var	See Biometric encoding of EF.DG3

4.12.1 Biometric Encoding of EF.DG3

DG3 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and is in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of [ISO/IEC 7816-11] MUST be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1. The number of instances in DG3 can be '0...n'.

Each nested template has the following structure:

Table 47: Data Group 3 Nested Tags

Tag	L	Value				
7F61	Var	Biometric Information Template Group Template				
		Tag	**L**	**Value**		
		02	01	Integer — Number of instances of this type of biometric		
		7F60	Var	1st Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype REQUIRED for DG3
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)

Tag	**L**	**Value**				
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	
		Tag	**L**			
		7F60	Var	2nd Biometric Information Template		
			Tag	**L**		
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype REQUIRED for DG3
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

The default OID of CBEFF is used. The OID data object (Tag ’06’) just under Biometric Information Template (BIT, Tag ’7F60’) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the Tag allocation Authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-4].

Note: ISO/IEC 39794 will succeed ISO/IEC 19794:2005 as international standard for encoding biometrics. See Part 10 Section 4.5.6.

4.12.2 DATA GROUP 3 — EF.DG3 Data Elements

This section describes the Data Elements that may be present in Data Group 3 (DG3). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 48: Data Elements for DG3

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If encoded finger(s) feature recorded)	Number of finger(s) biometric encodings recorded	1	F	N	0 to n identifying number of unique encodings of data on the finger(s).
02	M (If encoded finger(s) feature recorded)	Header		Var	B	Data Element may recur as defined by Data element 01.
03	M (If encoded finger(s) feature recorded)	Finger biometric data encoding(s)		Var	B	Data Element may recur as defined by Data element 01.

4.12.2.1 Biometric sub-type encoding

The biometric header template Tags and their assigned values are the minimum each implementation SHALL support as shown in the following table. Each single biometric information template has the following structure:

Table 49: Encoding of Sub-Features Scheme for the Encoding of Sub-Features: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
			0	0	0			No meaning
			0	0	1			Thumb
			0	1	0			Pointer
			0	1	1			Middle
			1	0	0			Ring
			1	0	1			Little
X	X	X						Reserved for future use

4.12.2.2 Encoding of Zero Instance

States not issuing LDS1 eMRTDs with fingerprints SHOULD NOT populate DG3. Data Group 3 of this structure has the drawback that it will result in a static DG3 hash in the SO_D for all LDS1 eMRTDs where the biometric features are not present and populated at the time of LDS1 eMRTD issuance, but the DG3 is declared. For interoperability purposes States supporting fingerprints in their LDS1 eMRTDs MUST store an empty Biometric Information Group Template in cases where no fingerprints are available at the time of LDS1 eMRTD issuance. The template counter denotes a value of '00' in this case.
It is RECOMMENDED to add Tag '53' with issuer defined content (e.g. a random number).

Table 50: Encoding Zero Instances

Tag	**L**	**Value**				
63	Var	LDS element				
		Tag	**L**	**Value**		
		7F 61	03	Biometric Information Group Template		
			02	01	00	Defines that there are no Biometric Information Templates stored in this Data Group.
		53	Var	Issuer defined content (e.g. a random number).		

4.12.2.3 Encoding of One Instance

In cases where only one fingerprint is available, the single instance MUST be encoded in the following manner (example for DG3 – fingerprint):

Table 51: Encoding One Instance

Tag	**L**	**Value**						
63	Var	LDS element where aa is the total length of the entire LDS data content						
		Tag	**L**	**Value**				
		7F 61	Var	Biometric Information Group Template.				
			02	01	01	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
			7F 60	Var	First biometric information template where cc is the total length of the entire BIT			
				A1	Var	Biometric Header Template.		
					81	01	08	Biometric type "Fingerprint"
					82	01	0A	Biometric subtype "left pointer finger"
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. Of course, this fingerprint can either be a left or right finger depending on the available image.			
				5F 2E	Var	Biometric Data. The Biometric Data Block MUST contain exactly one fingerprint image.		

Note: ISO/IEC 39794 will succeed ISO/IEC 19794:2005 as international standard for encoding biometrics. See Part 10

Section 4.5.6.

4.12.2.4 Encoding of More than One Instance

To achieve interoperability each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available. The following table contains a worked example for the CBEFF encoding of an interoperable DG 3 element with two fingerprint images.

Table 52: Encoding Greater than One Instance

Tag	**L**	**Value**						
63	Var	LDS element where *aa* is the total length of the entire LDS data content.						
		Tag	**L**	**Value**				
		7F 61	Var	Biometric Information Template Group Template.				
			02	01	02	Defines the total number of fingerprints stored as Biometric Information Templates that follow.		
			7F 60	Var	First biometric information template.			
				A1	Var	Biometric Header Template.		
					81	01	08	Biometric type “Fingerprint”
					82	01	0A	Biometric subtype “left pointer finger”
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
				5F 2E	Var	Biometric Data Block.The Biometric Data Block MUST contain exactly one fingerprint image.		
			7F 60	Var	Second biometric information template.			
				A1	Var	Biometric Header Template.		
					81	01	08	Biometric type “Fingerprint”
					82	01	09	Biometric subtype “right pointer finger”

Tag	L	Value						
					87	02	01 01	Format Owner JTC 1 SC 37
					88	02	00 07	Format Type [ISO/IEC 19794-4]
					Note that the BHT may contain additional optional elements. It is also possible that the order of fingerprints (left/right) is different.			
				5F 2E	Var	Biometric Data Block. The Biometric Data Block MUST contain exactly one fingerprint image.		

Note: ISO/IEC 39794 will succeed ISO/IEC 19794:2005 as international standard for encoding biometrics. See Part 10 Section 4.5.6.

4.13 DATA GROUP 4 — Additional Identification Feature — Iris(es) (OPTIONAL)

ICAO recognizes that member States may elect to use iris recognition as additional biometric technologies in support of machine assisted identity confirmation, which SHALL be encoded as Data Group 4 (DG4).

Table 53: Data Group 4 Tags

Tag	L	Value
76	Var	See Biometric encoding of EF.DG4

4.13.1 Biometric Encoding of EF.DG4

DG4 MUST use the Biometric Information Template (BIT) group template with nested BITs specified in [ISO/IEC 7816-11], which allows the possibility to store multiple biometric templates and is in harmony with the Common Biometric Exchange File Format (CBEFF). The biometric sub-header defines the type of biometric that is present and the specific biometric feature. The nested option of ISO/IEC [7816-11] MUST be used, even for encodings of a single biometric template. The latter case is indicated by numbering with n=1. The number of instances in DG4 can be '0...n'.

Each nested template has the following structure:

Table 54: Data Group 4 Nested Tags

Tag	L	Value				
7F61	Var	Biometric Information Template Group Template				
		Tag	**L**	**Value**		
		02	1	Integer — Number of instances of this type of biometric		
		7F60	Var	1st Biometric Information Template		
			Tag	**L**	**Value**	
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version '0101' (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric sub-type, REQUIRED for DG4
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)

Tag	**L**	**Value**				
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	
		Tag	**L**	**Value**		
		7F60	Var	2nd Biometric Information Template		
			Tag	**L**	**Value**	
			A1	Var	Biometric Header Template (BHT)	
				Tag	**L**	**Value**
				80	02	ICAO header version ‘0101’ (Optional) — Version of the CBEFF patron header format
				81	01-03	Biometric type (Optional)
				82	01	Biometric subtype REQUIRED for DG4
				83	07	Creation date and time (Optional)
				85	08	Validity period (from through) (Optional)
				86	04	Creator of the biometric reference data (PID) (Optional)
				87	02	Format owner (REQUIRED)
				88	02	Format type (REQUIRED)
			5F2E or 7F2E	Var	Biometric data (encoded according to Format Owner) also called the biometric data block (BDB).	

The default OID of CBEFF is used. The OID data object (Tag ’06’) just under Biometric Information Template (BIT, Tag ’7F60’) specified in [ISO/IEC 7816-11] is not included in this structure. Likewise the Tag allocation authority is not specified in the structure.

To facilitate interoperability, the first biometric recorded in each Data Group SHALL be encoded as per [ISO/IEC19794-6].

Note: ISO/IEC 39794 will succeed ISO/IEC 19794:2005 as international standard for encoding biometrics. See Part 10 Section 4.5.6.

4.13.2 DATA GROUP 4 — EF.DG4 Data Elements

This section describes the Data Elements that may be present in Data Group (DG4). Data Elements and their format within each Data Group area SHALL be as in the following table:
Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 55: Data Elements for DG4

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if encoded eye(s) feature included	Number of eye biometric encodings recorded	1	F	N	1 to 9 identifying number of unique encodings of data on the eye(s).
02	M, if encoded eye(s) feature included	Header		Var	B	Data Element may recur as defined by Data element 01.
03	M, if encoded eye(s) feature included	Eye biometric data encoding(s)		Var	B	Data Element may recur as defined by Data element 01.

4.13.2.1 Biometric Sub-Type Encoding

The biometric header template Tags and their assigned values are the minimum each implementation SHALL support as shown in the following table. Each single biometric information template has the following structure:

Table 56: Encoding of sub-features scheme for the encoding of sub-features: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Sub-type
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
			0	0	0			Reserved for future use
			0	0	1			Reserved for future use
			0	1	0			Reserved for future use
			0	1	1			Reserved for future use
			1	0	0			Reserved for future use
			1	0	1			Reserved for future use
X	X	X						Reserved for future use

4.13.2.2 Encoding of Zero Instance

States not issuing LDS1 eMRTDs with irises SHOULD NOT populate DG4. Data Group 4 of this structure has the drawback that it will result in a static DG4 hash in the SO_D for all LDS1 eMRTDs where the biometric features are not present and populated at the time of LDS1 eMRTD issuance but the DG4 is declared. For interoperability purposes States supporting irises in their LDS1 eMRTDs MUST store an empty Biometric Information Group Template in cases where no irises are available at the time of LDS1 eMRTD issuance. The template counter denotes a value of '00' in this case.

It is RECOMMENDED to add Tag '53' with issuer defined content (e.g. a random number).

Table 57: Encoding Zero Instances

<table>
<tr><th>Tag</th><th>L</th><th colspan="5">Value</th></tr>
<tr><td>76</td><td>Var</td><td colspan="5">LDS element</td></tr>
<tr><td></td><td></td><td>Tag</td><td>L</td><td colspan="3">Value</td></tr>
<tr><td></td><td></td><td>7F 61</td><td>03</td><td colspan="3">Biometric Information Template Group Template</td></tr>
<tr><td></td><td></td><td></td><td>02</td><td>01</td><td>00</td><td>Defines that there are no Biometric Information Templates stored in this Data Group.</td></tr>
<tr><td></td><td></td><td>53</td><td>Var</td><td colspan="3">Issuer defined content (e.g. a random number).</td></tr>
</table>

4.13.2.3 Encoding of One Instance

In cases where only one iris is available, the single instance MUST be encoded.

4.13.2.4 Encoding of More than One Instance

To achieve interoperability each feature MUST be stored in an individual Biometric Information Template. The feature position MUST be specified within the CBEFF biometric subtype if this information is available.

4.14 DATA GROUP 5 — Displayed Portrait (OPTIONAL)

Data Elements assigned to Data Group 5 (DG5) SHALL be as follows:

Table 58: Data Group 5 Tags

Tag	**L**	**Value**		
65	Var			
		Tag	**L**	**Value**
		02	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		5F40	Var	Displayed portrait

The following format owners are recognized for the specified type of displayed image.

Table 59: DG5 Formats

Displayed Image	Format Owner
Displayed Facial Image	[ISO/IEC 10918], JFIF option

4.14.1 DATA GROUP 5 — EF.DG5 Data Elements (Optional)

This section describes the Data Elements that may be present in Data Group 5 (DG5). Data Elements and their format within Data Group 5 SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 60: Data Elements for DG5

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed portrait recorded)	Number of displayed portraits recorded	1	F	N	1 to 9 identifying number of unique recordings of displayed portrait.
02	M (If displayed portrait recorded)	Displayed portrait representation(s)		Var	A,N	Data Element may recur as defined by Data element 01.
03	M (If displayed portrait recorded)	Number of bytes in representation of displayed portrait	5	F	N	00001 to X9, identifying number of bytes in representation of displayed portrait immediately following.
04	M (If displayed portrait recorded)	Representation of displayed portrait		Var	B	Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

Note: Data Element 02 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

4.15 DATA GROUP 6 — Reserved for Future Use

Data Elements assigned to Data Group 6 (DG6) SHALL be as follows:

Table 61: Data Group 6 Tags

Tag	L	Value
66	Var	

4.15.1 DATA GROUP 6 — EF.DG6 Data Elements

The data elements for Data Group 6 (DG6) are reserved for future use.

4.16 DATA GROUP 7 — Displayed Signature or Usual Mark (OPTIONAL)

Data Elements assigned to Data Group 7 (DG7) SHALL be as follows:

Table 62: Data Group 7 Tags

Tag	L	Value		
67	Var			
		Tag	**L**	**Value**
		02	Var	Number of instances of this type of displayed image (REQUIRED in first template. Not used in succeeding templates.)
		5F43	Var	Displayed Signature

The following format owners are recognized for the specified type of displayed image:

Table 63: DG7 Formats

Displayed Image	Format Owner
Displayed Signature/usual mark	[ISO/IEC 10918], JFIF option

4.16.1 DATA GROUP 7—EF.DG7 Data Elements (OPTIONAL)

This section describes the Data Elements that may be present in Data Group 7 (DG7). Data Elements and their format within each Data Group 7 SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 64: Data Elements for DG7

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If displayed signature or usual mark recorded)	Number of displayed signature or usual marks	1	F	N	1 to 9 identifying number of unique recordings of displayed signature or usual mark.
02	M (If displayed signature or usual mark recorded)	Displayed signature or usual mark representation		Var	B	Data Element may recur as defined by DE 01. Formatted as per [ISO/IEC 10918-1] or [ISO/IEC 15444].

Note: Data Element 02 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option, or [ISO/IEC 15444] using JPEG 2000 image coding system.

4.17 DATA GROUP 8 — Data Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, they are available for temporary proprietary usage. This Data Element could use a structure similar to that for biometric templates, machine assisted security feature verification and encoded detail(s). Data Elements combining to form Data Group 8 (DG8) SHALL be as follows:

Table 65: Data Group 8 Tags

Tag	**L**	**Value**		
68	Var	To Be Defined		
		Tag	**L**	**Value**
		02	1	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	Header Template. Details to be defined.

4.17.1 DATA GROUP 8 — EF.DG8 Data Elements

This section describes the Data Elements that may be present in Data Group 8 (DG8). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 66: Data Elements for DG8

Data Element	**Optional or MANDATORY**	**Name of Data Element**	**Number of Bytes**	**Fixed or Variable**	**Type of Coding**	**Coding Requirements**
01	M (If this encoded feature is used)	Number of data feature(s)	1	F	N	1 to 9, identifying number of unique encodings of data feature(s) (embraces Data element 02 through 03).
02	M (If this encoded feature is used)	Header (to be defined)	1			Header details to be defined.
03	M (If this encoded feature is used)	Data feature(s) data	999 Max	Var	A,N,S,U ,B	Format defined at the discretion of issuing State or organization.

4.18 DATA GROUP 9 — Structure Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, it is available for temporary proprietary use. These Data Elements could use a structure similar to that for biometric templates. Data Elements combining to form Data Group 9 (DG9) SHALL be as follows:

Table 67: Data Group 9 Tags

Tag	L	Value		
69	Var	To Be Defined		
		Tag	**L**	**Value**
		02	01	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			X	Header Template. Details to be defined.

4.18.1 DATA GROUP 9 — EF.DG9 Data Elements

Data Group 9 (DG9) Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 68: Data Elements for DG9

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of structure feature(s)	1	F	N	1 to 9, identifying number of unique encodings of structure feature(s) (embraces Data element 02 through 03).
02	M (If this encoded feature is used)	Header (to be defined)			N	Header details to be defined
03	M (If this encoded feature is used)	Structure feature(s) data		Var	B	

4.19 DATA GROUP 10 — Substance Feature(s) (OPTIONAL)

This Data Group has yet to be defined. Until then, it is available for temporary proprietary usage. These Data Elements could use a structure similar to that for biometric templates. Data Elements combining to form Data Group 10 (DG10) SHALL be as follows:

Table 69: Data Group 10 Tags

Tag	L	Value		
6A	Var			
		Tag	**L**	**Value**
		02	01	Integer — Number of instances of this type of template (REQUIRED in first template. Not used in succeeding templates.)
			Var	To Be Defined.

4.19.1 DATA GROUP 10 — EF.DG10 Data Elements

This section describes the Data Elements that may be present in Data Group 10 (DG10). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 70: Data Elements for DG10

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M (If this encoded feature is used)	Number of substance feature(s) recorded	1	F	N	1 to 9, identifying number of unique encodings of substance feature(s) (embraces Data element 02 through 03).
02	M (If this encoded feature is used)	Header (to be defined)	TBD	TBD	N	Details to be defined.
03	M (If this encoded feature is used)	Substance feature(s) data	999 Max	Var	A,N,S,U ,B	Format defined at the discretion of issuing State or organization.

4.20 DATA GROUP 11 — Additional Personal Detail(s) (OPTIONAL)

This Data Group is used for additional details about the document holder. Since all of the Data Elements within this group are optional, a Tag list is used to define those present. Data Elements combining to form Data Group 11 (DG11) SHALL be as follows:

Note:This template may contain non-Latin characters.

Table 71: Data Group 11 Tags

Tag	**L**	**Value**				
6B	Var					
		Tag	**L**	**Value**		
		5C	Var			Tag list with list of Data Elements in the template.
		5F0E	Var			Full name of document holder in national characters. Encoded per Doc 9303 rules.
		A0	Var			Content-specific class
				Tag	**L**	**Value**
				02	01	Number of other names
				5F0F	Var	Other name formatted per Doc 9303. The data object repeats as many times as indicated in number of other names (data object with Tag'02')
		Tag	**L**	**Value**		
		5F10	Var			Personal number
		5F2B	08			Full date of birth yyyymmdd
		5F11	Var			Place of birth. Fields separated by '<'
		5F42	Var			Permanent address. Fields separated by '<'
		5F12	Var			Telephone
		5F13	Var			Profession
		5F14	Var			Title
		5F15	Var			Personal summary
		5F16	Var			Proof of citizenship. Compressed image per [ISO/IEC 10918]
		5F17	Var			Other valid TD numbers. Separated by '<'
		5F18	Var			Custody information

4.20.1 DATA GROUP 11 — EF.DG11 Data Elements

This section describes the Data Elements that may be present in Data Group 11 (DG11). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note 1: Data Element 11 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

Note 2: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 72: Data Elements for DG11

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Name of holder (in full)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
02	O	Other name(s)	99 Max	Var	B	Filler characters (<) inserted as per MRZ. No fillers inserted at end of line. Truncation not permitted.
03	O	Personal number	99 Max	Var	U	Free-form text.
04	O	Full date of birth	8	F	N	YYYYMMDD
05	O	Place of birth	99 Max	Var	U	Free-form text.
06	O	Address	99 Max	Var	U	Free-form text.
07	O	Telephone	99 Max	Var	N,S	Free-form text. Encoding per ITU-T E.164 recommended
08	O	Profession	99 Max	Var	U	Free-form text.
09	M, if Data element 08 included	Title	99 Max	Var	U	Free-form text.
10	M, if Data element 09 included	Personal summary	99 Max	Var	U	Free-form text.
11	M, if Data element 10 included	Proof of citizenship		Var	B	Image of citizenship document formatted as per [ISO/IEC 10918-1]
12	O	Other valid travel	99	Var	U	Free-form text, separated

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
		document(s) Travel document number	Max			by <.
13	O	Custody information	999 Max	Var	U	Free-form text.

Note: In case the month (MM) or the day (DD) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '00'. In case the century and the year (CCYY) are unknown, the interoperable way to indicate this in DG11 is to set the respective characters to '0000'. Issuer-assigned dates MUST always be used consistently.

4.21 DATA GROUP 12 — Additional Document Detail(s) (OPTIONAL)

This Data Group is used for additional information about the document. All Data Elements within this group are optional.

Table 73: Data Group 12 Tags

Tag	**L**	**Value**				
6C	Var					
		Tag	**L**	**Value**		
		5C	Var			Tag list with list of Data Elements in the template.
		5F19	Var			Issuing Authority
		5F26	08			Date of issue. yyyymmdd
		A0	Var			Content-specific class
				Tag	**L**	**Value**
				02	01	Number of other persons
				5F1A	Var	Name of other person formatted per Doc 9303 rules. The data object repeats as many times as indicated in number of other names Data element 02 (data object with Tag'02').
		Tag	**L**	**Value**		
		5F1B	Var			Endorsements, observations
		5F1C	Var			Tax/Exit requirements
		5F1D	Var			Image of front of document. Image per ISO/IEC 10918
		5F1E	Var			Image of rear of document. Image per ISO/IEC 10918
		5F55	0E			Date and time of document personalization yyyymmddhhmmss
		5F56	Var			Serial number of personalization system

It is RECOMMENDED that Inspection Systems support both 8 bytes ASCII and BCD date/time encoding.

4.21.1 DATA GROUP 12 — EF.DG12 Data Elements

This section describes the Data Elements that may be present in Data Group 12 (DG12). Data Elements and their format within each Data Group SHALL be as in the following table:

Note 1: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Note 2: Data Elements 07 and 08 SHALL be encoded as defined in [ISO/IEC 10918], using the JFIF option or [ISO/IEC 15444] using JPEG 2000 image coding system.

Table 74: Data Elements for DG12

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	O	Issuing Authority	99 Max	Var	U	Free-form text.
02	O	Date of issue	8	F	N	Date of issue of document; i.e. YYYYMMDD.
03	O	Other person(s) details	99 Max	Var	U	Free-form text
04	O	Endorsement(s)/ Observation(s)	99 Max	Var	U	Free-form text.
05	O	Tax/Exit requirements	99 Max	Var	U	Free-form text.
06	O	Image of front of eMRTD		Var	B	Formatted as per [ISO/IEC 10918-1]
07	O	Image of rear of MRTD		Var	B	Formatted as per [ISO/IEC 10918-1]
08	O	Personalization Time	14	F	N	yyyymmddhhmmss
09	O	Personalization device serial number	99 max	Var	U	Free format.

4.22 DATA GROUP 13 — Optional Details(s) (OPTIONAL)

Data Elements combining to form Data Group 13 (DG13) are at the discretion of the issuing State or organization and SHALL be as follows:

Table 75: Data Group 13 Tags

Tag	L	Value
'6D'	Var	

4.23 DATA GROUP 14 — Security Options (CONDITIONAL)

Data Group 14 contains security options for additional security mechanisms. For details see Doc 9303-11. The file DG14 contained in the ePassport Application is REQUIRED if Chip Authentication or PACE-GM/-IM is supported by the eMRTD chip.

Table 76: Data Group 14 Tags

Tag	L	Value
6E	Var	Refer to Doc 9303-10 Data Group 14 SecurityInfos

4.23.1 DATA GROUP 14 — EF.DG14 Data Elements

This section describes the Data Elements that may be present in Data Group 14 (DG14). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 77: Data Elements for DG14

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	SecurityInfos		Var	B	Refer to Doc 9303-10. Data Group 14 SecurityInfos as defined in 4.23.2

4.23.2 DATA GROUP 14 SecurityInfos

The following generic ASN.1 data structure SecurityInfos allows various implementations of security options for secondary biometrics. For interoperability reasons, it is RECOMMENDED that this data structure be provided by the eMRTD chip in DG14 to indicate supported security protocols. The data structure is specified as follows:

```
SecurityInfos ::=    SET of SecurityInfo

SecurityInfo  ::=    SEQUENCE {
       protocol            OBJECT IDENTIFIER,
       requiredData  ANY DEFINED BY protocol,
       optionalData  ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a SecurityInfo data structure have the following meaning:

- The object identifier protocol identifies the supported protocol;
- The open type requiredData contains protocol specific mandatory data;
- The open type optionalData contains protocol specific optional data.

4.24 DATA GROUP 15 — Active Authentication Public Key Info (CONDITIONAL)

This OPTIONAL Data Group contains the Active Authentication Public Key and is REQUIRED when implementing the optional Active Authentication chip authentication as described in Doc 9303-11.

Table 78: Data Group 15 Tags

Tag	L	Value
6F	Var	Refer to Doc 9303-11

4.24.1 DATA GROUP 15 — EF.DG15 Data Elements

This section describes the Data Elements that may be present in Data Group 15 (DG15). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 79: Data Elements for DG15

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
	O	ActiveAuthenticationPublicKeyInfo		Var	B	See Doc 9303-11

4.25 DATA GROUP 16 — Person(s) to Notify (OPTIONAL)

This Data Group lists emergency notification information. It is encoded as a series of templates using the Tag 'Ax' designation. DG16 (as all other Data Groups) SHOULD not be updated after issuance; DG16 is represented by a hash value in the SO_D and the SO_D is only signed once at issuance.

Table 80: Data Group 16 Tags

Tag	L	Value		
70	Var			
		Tag	**L**	**Value**
		02	01	Number of templates (occurs only in first template)
		Ax	Var	Start of template, where x (x=1,2,3…) increments for each occurrence
5F50	08			Date data recorded
5F51	Var			Name of person
5F52	Var			Telephone
5F53	Var			Address

4.25.1 DATA GROUP 16 — EF.DG16 Data Elements

This section describes the Data Elements that may be present in Data Group 16 (DG16). Data Elements and their format within each Data Group area SHALL be as in the following table:

Note: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character ['<'], B = Binary data, F = fixed-length field, Var = variable-length field.

Table 81: Data Elements for DG16

Data Element	Optional or MANDATORY	Name of Data Element	Number of Bytes	Fixed or Variable	Type of Coding	Coding Requirements
01	M, if DG 16 included	Number of persons identified	1	F	N	Identifies number of persons included in the Data Group.
02	M, if DG 16 included	Date details recorded	8	F	N	Date notification date recorded; Format = YYYYMMDD.
03	M, if DG 16 included	Name of person to notify Primary and secondary identifiers		Var	A,N,S	Filler characters (<) inserted as per MRZ. Truncation not permitted.
04	M, if Data element 03 included	Telephone number of person to notify		Var	N,S	Telephone number in international form (country code and local number). Encoding per ITU-T E.164 recommended.
05	M	Address of person to notify		Var	U	Free-form text.

5 LDS 2 APPLICATIONS (OPTIONAL)

Logical Data Structure 2 (LDS2) is an optional and backwards compatible extension to the LDS1 eMRTD chip that would allow for the digital and secure storage of travel information, after the document has been issued. LDS2 extends the use of the ePassport through the addition of applications that could allow for the digital storage of travel data (visas and travel stamps), and other information that could facilitate the travel of the holder (additional biometrics), over its validity period. Better leveraging the full potential of the ePassport by 'digitizing' the remainder of the data contained in the documents offers a suite of facilitation benefits, while further protecting the document against vulnerabilities such as counterfeiting, copying and unauthorized reading or writing.

The additional and optional applications described as LDS 2 are:

- Travel Records (Stamps);
- Electronic Visas; and
- Additional Biometrics.

It is MANDATORY for the LDS1 eMRTD application to be present before any OPTIONAL LDS2 applications may be declared.

5.1 Travel Records Application (CONDITIONAL)

The Travel Records application MAY be implemented by an issuing State or organization. The following is conditionally REQUIRED if the optional Travel Records application has been invoked.

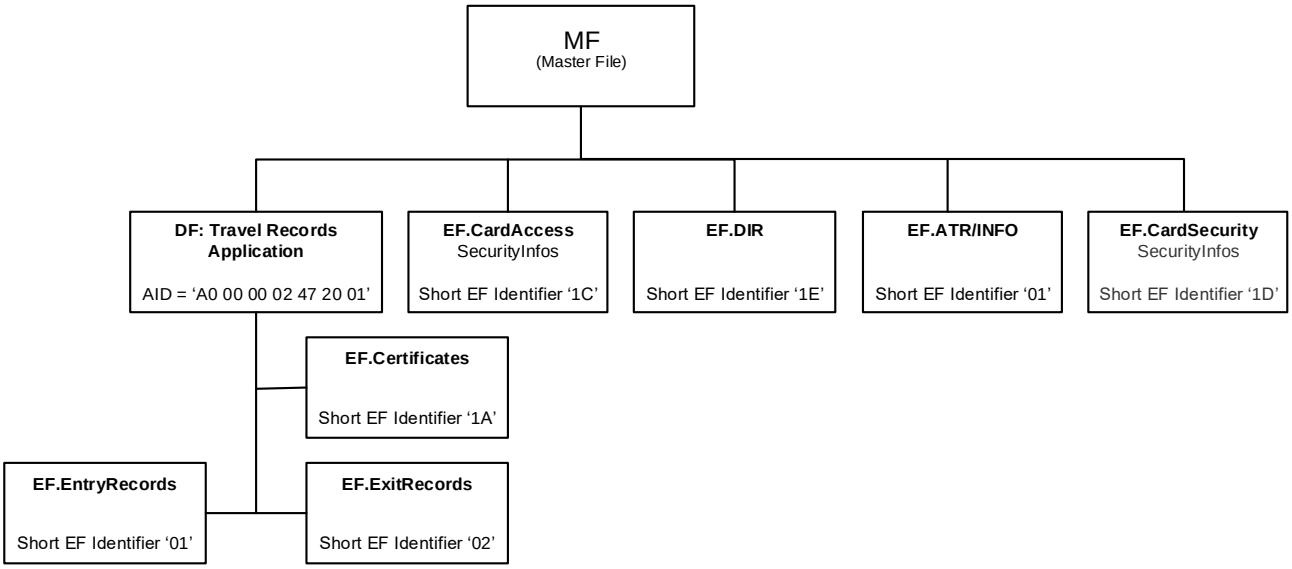


Figure 4: Travel Records Structure

Entry and Exit Travel Records are stored in two separate Elementary Files EF.EntryRecords and EF.ExitRecords under the Travel Records application DF with both having Linear Structure with Records of Variable Size as per [ISO/IEC 7816-4]. Travel Records Signer certificates are stored in a separate Elementary File EF.Certificates having Linear Structure with Records of Variable Size.

5.1.1 Application Selection -DF

The Travel Records application MUST be selected by use of the Application Identifier (AID) as a reserved DF name. The AID MUST consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] followed by the Proprietary Application Identifier Extension (PIX) of the Travel Records application:

- The Registered Application Identifier is 'A0 00 00 02 47';
- The Travel Records application MUST use PIX = '20 01';
- The full AID of the Travel Records application MUST be A0 00 00 02 47 20 01.

If the effective authorization does not grant access rights to any data in a LDS2 Application, selecting this application MUST be rejected by the IC.

5.1.2 EF.Certificates (MANDATORY)

The Travel Records Signer certificates are stored in an EF inside the application DF and having Linear Structure with Records of Variable Size. These certificates are intended to be used by the IS to further offline validation of the digital signatures for each record in both the EF.ExitRecords and EF.EntryRecords files.

Table 82: EF.Certificates

File Name	EF.Certificates
File ID	'011A'
Short EF Identifier	'1A'
Select / FMM Access	PACE+TA (Travel record authorization bit b3 according to Table 96)
Read record / Search Record Access	PACE+TA (Travel record authorization bit b3 according to Table 96)
Append Record Access	PACE+TA (Travel record authorization bit b4 according to Table 96)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

Certificate record contains a single LDS2-TS Signer X.509 certificate data object. A Certificate record MAY be referenced by one or more Entry or Exit Travel Record.

Table 83: EF.Certificates Record Format

Tag	Content	Mandatory /Optional	Format	Example
5F3A	Certificate serial number	M	V(22)B	'5F3A' 'Len' {Country code || SerialNumber }
72	X.509 certificate	M	V (900) B	'72' Len { X.509 Certificate }

Note: Interindustry tags specified in this table are used in LDS context, so coexistent tag allocation scheme is not required.

DO '5F3A' MUST contain a 2 letter country code according to Doc 9303 Part 3 (same encoding and value as X.509 certificate's subject's countryName) followed by the certificate serial number.

Each X.509 certificate contains a set of ASN.1 encoded data elements illustrated in Table 84. Detailed requirements for the X.509 Certificate can be found in Doc 9303-12 Certificate Profile Specification.

Table 84: X.509 Certificate Structure Example

Field			Description	Example value
Certificate				
	version		Must be ver.3	2
	serialNumber		unique positive integer	20 bytes max
	signature		Signature algorithm	ecdsa-with-SHA256
	issuer			
		countryName	Issuing country name	"US"
		commonName	Issuer name (9 chars max)	"DHSCA0001"
	validity			
		notBefore	Cert. effective date	"131225000000Z"
		notAfter	Cert. expiration date	"230824235959Z"
	subject			
		countryName	IS country name	"US"
		commonName	IS name (9 chars max)	"SFO000001"
	subjectPublicKeyInfo			
		Public Key Algorithm	ecPublicKey	
		Subject Public Key	IS public key	ECC256 Public Key
	extensions			
		AuthorityKeyIdentifier		
		ExtKeyUsage		
Signature Algorithm			ecdsa-with-SHA256	
Signature			Issuer's Signature	ECDSA256 signature

Note: This table is an example for illustration only. Certificate records are written to EF.Certificates located under the Travel Records application DF using the APPEND RECORD command. Certificate records can be read from EF.Certificates using READ RECORD command. Certificate records MUST NOT be updated or erased. The maximum number of records in EF.Certificates under the Travel Records application DF MUST be 254.

5.1.3 EF.ExitRecords (MANDATORY)

Exit Records MUST be appended by an authorized IS upon embarkation.

Table 85: EF.ExitRecords

File Name	EF.ExitRecords
File ID	'0102'
Short EF Identifier	'02'
Select / FMM Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Read Record / Search Record Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Append Record Access	PACE+TA (Travel record authorization bit b2 according to Table 96)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

The content of an Exit Record is shown in Table 86.

Note: Interindustry tags specified in the table below are used in LDS context, so coexistent tag allocation

scheme is not required.

Table 86: Entry / Exit Record Format

Tag	Tag	Content	Mandatory /OPTIONAL	Format	Example
5F44		Embarkation/Debarkation State (copy for SEARCH RECORD)	M	F (3) A	USA
73		Entry / Exit Travel Record (signed info)			
	5F44	Embarkation/Debarkation State	M	F (3) A	USA
	5F4C	Visa approvals, refusals, and revocations	O	V (50) A,N,S,U	Free-form text
	5F45	Travel date (Date of entry/exit)	M	F (8) N	20120814 (yyyymmdd)
	5F4B	Inspection authority	M	V (10) A,N,S	CBP
	5F46	Inspection location (Port of Entry/Exit)	M	V (10) A,N,S	SFO
	5F4A	Inspector reference	M	V (20) A,N,S	SFO00001234
	5F4D	Result of inspection	O	V (50) A,N,S,U	Free-form text
	5F49	Mode of travel	O	F (1) A	A (Air), S (Sea), L (Land)
	5F48	Duration of stay (days)	O	V (2) B	‘00FF’ (255 days)
	5F4E	Conditions holder is required to observe whilst in issuing State	O	V(50) A,N,S,U	Free-form text
5F37		Authenticity token (Signature)	M	V (140) B	‘5F’ ‘37’ Len {Signature}
5F38		Reference (record number) to LDS2-TS Signer certificate in Certificates Store	M	F (1) B	‘01’ …’FE’

Note 1: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character [‘<’ ‘ ’], B = Binary data, F = fixed-length field, V = variable- length field.

Note 2: Since LDS2-TS Signer certificates are likely to be the same in multiple Travel Records (ex., when entering and exiting a country through the same airport having only one LDS2-TS Signer), before writing/appending a new certificate to the EF.Certificates, the IS should look up the EF.Certificates for a copy of the same certificate, and reference the existing one. This will reduce the size of EF.Certificates and enable faster lookups.

Note 3: The LDS2 eMRTD does not enforce that an IS writes Entry Records only to the EF.EntryRecords, but not to the EF.ExitRecords, and vice versa.

Note 4: Embarkation/Debarkation State 3-letter code according to Doc9303-3.

The order of the data objects in a record is fixed. The IS MUST build up the record content using the data objects in the order specified in the table.

Each Record MUST contain a digital signature (Authenticity Token) calculated over the DO’73, including Tag 73 and Length. Signature is generated by the LDS2-TS Signer.

LDS2-TS Signer certificates required to verify Travel Record’s signature MUST be stored in the EF.Certificates under the Travel Records application DF if not already available in the same file.

Travel Records are written (appended) to EF using APPEND RECORD. Travel Records MUST NOT be altered (updated) or deleted. The maximum number of records in each EF allowed MUST be 254.

5.1.4 EF.EntryRecords (MANDATORY)

Entry Records MUST be appended by an authorized IS upon debarkation.

Table 87: EF.EntryRecords

File Name	EF.EntryRecords
File ID	’0101’
Short EF Identifier	’01’
Select / FMM Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Read Record / Search Record Access	PACE+TA (Travel record authorization bit b1 according to Table 96)
Append Record Access	PACE+TA (Travel record authorization bit b2 according to Table 96)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

The structure of the entry record is identical to the structure of the exit record specified in Table 86.

5.2 Visa Records Application (CONDITIONAL)

The Visa Records application MAY be implemented by an issuing State or organization. The following is conditionally REQUIRED if the optional Visa Records application has been invoked.

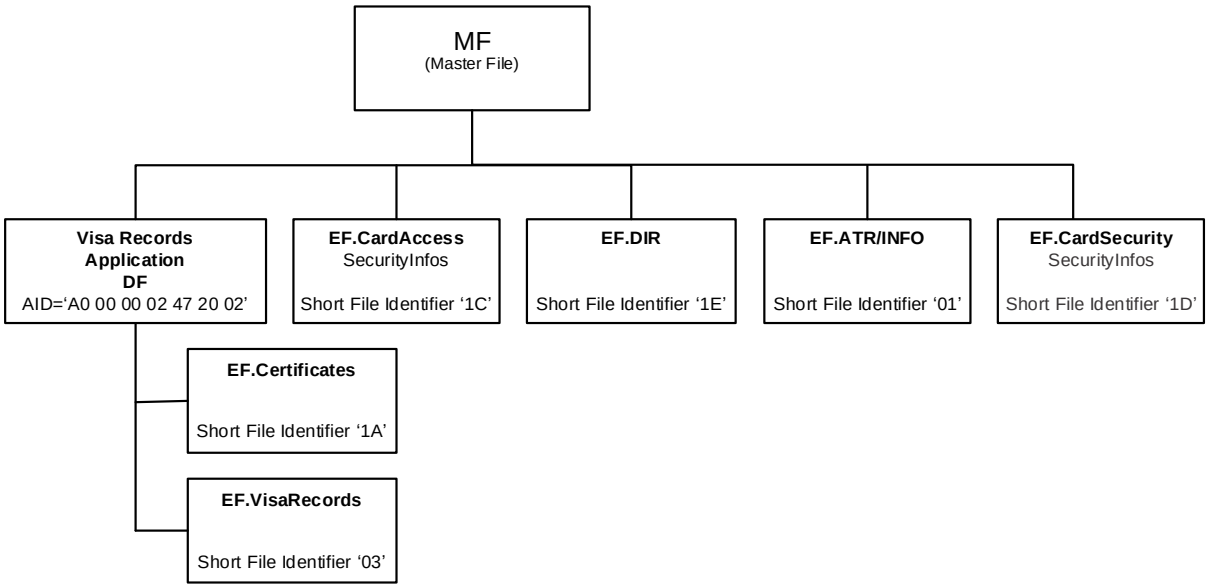


Figure 5: Visa Records Structure

Visa Records are stored in the Elementary File EF.VisaRecords under the Visa Records application DF. EF SHALL have Linear Structure with Records of Variable Size as per [ISO/IEC 7816-4]. Visa Records Signer certificates are stored in a separate Elementary File EF.Certificates having Linear Structure with Records of Variable Size.

5.2.1 Application Selection -DF

The Visa Records application MUST be selected by use of the Application Identifier (AID) as a reserved DF name. The AID MUST consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] followed by the Proprietary Application Identifier Extension (PIX) of the Visa Records application:

- The Registered Application Identifier is 'A0 00 00 02 47';
- The Visa Records application MUST use PIX = '20 02';
- The full AID of the Visa Records application is 'A0 00 00 02 47 20 02'.

If the effective authorization does not grant access rights to any data in a LDS2 Application, selecting this application MUST be rejected by the IC.

5.2.2 EF.Certificates (MANDATORY)

The Visa Records Signer certificates are stored in EF.Certificates inside the application DF and having linear structure with records of variable size. These certificates are intended to be used by the IS to further offline validation of the digital signature for each record in the EF.VisaRecords.

Table 88: EF.Certificates

File Name	EF.Certificates
File ID	’011A’
Short EF Identifier	’1A’
Select / FMM Access	PACE+TA (Visa record authorization bit b3 according to Table 97)
Read Record / Search Record Access	PACE+TA (Visa record authorization bit b3 according to Table 97)
Append Record Access	PACE+TA (Visa record authorization bit b4 according to Table 97)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

Certificate record contains a single LDS2-V Signer X.509 certificate data object. A Certificate Record MAY be referenced by one or more Visa Records.

The structure of the Certificate record in Visa Application is identical to the structure of the Certificate record in Travel Record Application specified in Table 83.

Certificate records are written to EF.Certificates located under the Visa Records application DF using APPEND RECORD command. Certificate records can be read from EF.Certificates using READ RECORD command. Certificate records MUST NOT be updated or erased. The maximum number of records in EF.Certificates under the Visa Records application DF MUST be 254.

5.2.3 EF.VisaRecords (MANDATORY)

Visa Records MUST be stored in EF.VisaRecords having Linear Structure with Records of Variable Size.

Table 89: EF.VisaRecords

File Name	EF.VisaRecords
File ID	’0103’
Short EF Identifier	’03’
Select / FMM Access	PACE+TA (Visa record authorization bit b1 according to Table 97)
Read Record / Search Record Access	PACE+TA (Visa record authorization bit b1 according to Table 97)
Append Record Access	PACE+TA (Visa record authorization bit b2 according to Table 97)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

Each Visa Record MUST contain a sequence of BER-TLV data objects (DO ‘5F28’ and DO ‘71’), followed by the Authenticity Token (Signature) DO and DO containing reference to LDS2-V Signer certificate in EF.Certificates. DO ‘71’ contains a set of DOs (fields) listed in the table below.

Note: Interindustry tags specified in the table below are used in LDS context, so coexistent tag allocation scheme is not required.

Table 90: EF.VisaRecords Format

Tag	Tag	Content	MANDATORY/ OPTIONAL/ CONDITIONAL	Format	Example
5F28		Issuing State or organization (Copy for SEARCH RECORD)	M	F (3) A	NLD
71		Visa Record (signed info)			
	5F28	Issuing State or organization	M	F (3) A	NLD
	43	Document Type	M	F (2) A,N,S	VS
	5F71	Machine-Readable Visa of Type A	O	F (48) A,N,S	
	5F72	Machine-Readable Visa of Type B	O	F (44) A,N,S	VCD<<DENT<<ARTHUR< PHILIP<<<<<<<<<<<
	5F73	Number of entries	O	V (1) B	‘01’ – ‘FF’
	5F74	Duration of stay (days, months, years)	O	F (3) B	‘010000’ – ‘FFFFFF’
	5F75	Passport number	O	F (9) A,N,S	XI85935F8
	5F76	Visa Type/class/category	O	V (4) B	
	5F77	Territory Information	O	V (8) B	
	49	Place of issuance (Issuing authority)	M	V (50) A, Sp	NEW YORK
	5F25	Effective Date (Date of issuance)	M	F (8) N	20120826 (yyyymmdd)
	5F24	Expiration Date	M	F (8) N	20130826 (yyyymmdd)
	5A	Document number	M	F (9) A,N,S	XI85935F8
	5F32	Additional information (endorsements: duration, limitations, and fees paid)	O	V (50) A,N,S,U	Free-form text
	5B	Name of holder (full name)	M	V (50) A, Sp	VAN DER STEEN MARIANNE LOUISE
	5F33	Primary Identifier (surname)	M	V (50) A, Sp	VAN DER STEEN
	5F34	Secondary Identifier (given name)	M	V (50) A, Sp	MARIANNE LOUISE
	5F35	Sex	M	F (1) A,S	F, M, or <
	5F2B	Date of birth	M	F (8) N,S	19870814 (yyyymmdd)
	5F2C	Nationality	M	F (3) A	NLD
	5F1F	MRZ	M	V (50) A,N,S	VAN<DER<STEEN<< MARIANNE<LOUISE
	5F40	Reference to Additional Biometrics EF	O	F (2) B	’0201’
5F37		Authenticity token (Signature)	M	V (140), B	‘5F’ ‘37’ Len {Signature}
5F38		Reference (record number) to LDS2-V Signer certificate in Certificates Store	M	F (1) B	‘01’ …’FE’

Note 1: A = Alpha character [a..z, A..Z], N = Numeric character [0..9], S = Special character [‘<’ ‘ ’], B = Binary data, F = fixed-length field, V = variable- length field, Sp=Space.

Note 2: Issuing state 3-letter code according to Doc9303-3.

Note 3: Optional DO’5F40, if present, MUST contain the 2 bytes identifier of the EF within the Additional

Biometrics application containing biometric data. This DO may only be used provided the Additional Biometrics application is present on the eMRTD.

The order of the data objects in a record is fixed. The IS MUST build up the record content using the data objects in the order specified in the table.

Each Visa Record MUST contain a digital signature (Authenticity Token) calculated over the DO'71, including Tag 71 and Length. Signature is generated by the LDS2-V Signer.

LDS2-V Signer certificates required to verify Visa Record's signature are stored in a separate EF.Certificates store located under the Visa Records application DF.

Each Visa Record MUST be appended to EF.VisaRecords using APPEND RECORD. Visa Records and MUST NOT be altered (updated) or erased. The maximum number of records allowed in EF.VisaRecords MUST be 254.

5.3 Additional Biometrics Application (CONDITIONAL)

The Additional Biometrics application MAY be implemented by an issuing State or organization. The following is conditionally REQUIRED if the optional Additional Biometrics application has been invoked or any visa record has referenced it.

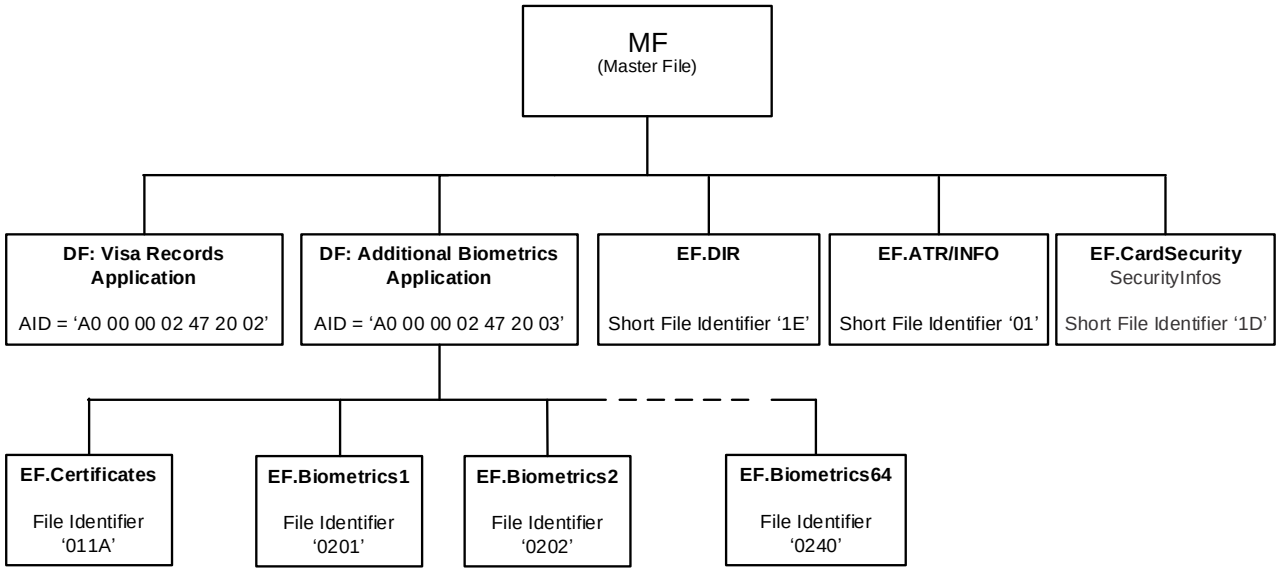


Figure 6: Additional Biometrics Application Structure

5.3.1 Application Selection -DF

The Additional Biometrics application MUST be selected by use of the Application Identifier (AID) as a reserved DF name. The AID MUST consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] followed by the Proprietary Application Identifier Extension (PIX) of the Additional Biometrics application:

- The Registered Application Identifier is 'A0 00 00 02 47';
- The Additional Biometrics application MUST use PIX = '20 03';
- The full AID of the Additional Biometrics application is 'A0 00 00 02 47 20 03'.

If the effective authorization does not grant access rights to any data in a LDS2 Application, selecting this application MUST be rejected by the IC.

5.3.2 EF.Certificates (MANDATORY)

The Additional Biometrics Signer certificates are stored in EF.Certificates inside the application DF and having linear structure with records of variable size. These certificates are intended to be used by the IS to further offline validation of the digital signature in the EF.Biometrics.

Table 91: EF.Certificates

File Name	EF.Certificates
File ID	’011A’
Short EF Identifier	’1A’
Select / FMM Access	PACE+TA (Additional Biometrics authorization byte 1 bit b1 (see Table 98)
Read Record/Search Record access	PACE+TA (Additional Biometrics authorization byte 1 bit b1 (see Table 98)
Append Record Access	PACE+TA (Additional Biometrics authorization byte 1 bit b2 (see Table 98)
Write / Update Record Access	NEVER
Erase Record Access	NEVER
File structure	Linear structure with records of variable size
Size	Variable

Certificate record contains a single Additional Biometrics Signer X.509 certificate data object. A Certificate Record MAY be referenced by one or more Additional Biometrics EF.

The structure of the Certificate record in Additional Biometrics Application is identical to the structure of the Certificate record in Travel Record Application specified in Table 83.

Certificate records are written to EF.Certificates located under the Additional Biometrics application DF using APPEND RECORD command. Certificate records can be read from EF.Certificates using READ RECORD command. Certificate records MUST NOT be updated or erased. The maximum number of records in EF.Certificates under the Additional Biometrics application DF MUST be 64.

5.3.3 EF.Biometrics

Additional Biometric MUST be stored under Additional Biometrics Application in EFs having Transparent Structure as per [ISO/IEC 7816-4].

Each Additional Biometrics EF MAY be linked to one or more records in EF.VisaRecords in Visa Records Application (or other EFs and applications) using Additional Biometrics EF Identifier.

Table 92: EF.Biometrics1…EF.Biometrics64

File Name	EF.Biometrics1……..EF.Biometrics64
File ID	’0201’ ... ‘0240’
Short EF Identifier	N/A
Select / FMM / Read Access in Deactivated state	PACE+TA (AdditionalBiometrics authorization according to Table 98, bits b2, b4, b6, b8 of byte 2 - 17)
Write Access in Deactivated state	PACE+TA (AdditionalBiometrics authorization according to Table 98, bits b2, b4, b6, b8 of byte 2 - 17)
Activate Access in Deactivated state	PACE+TA (AdditionalBiometrics authorization according to Table 98, bits b2, b4, b6, b8 of byte 2 - 17)
Select / FMM / Read Access in Activated state	PACE+TA (AdditionalBiometrics authorization according to Table 98, bits b1, b3, b5, b7 of byte 2 - 17)
Write Access in Activated state	NEVER
Activate Access in Activated state	NEVER
Erase Access	NEVER
File structure	Transparent structure
Size	Variable

Each Additional Biometric EF MUST contain a BER-TLV data object DO'7F2E encapsulating 3 data objects - the Biometric data DO'5F2E followed by the Authenticity Token (Signature) DO'5F37' and DO'5F38' containing the reference to an Additional Biometrics Signer certificate in EF.Certificates as shown in the table below.

The content of DO'5F2E is up to the Additional Biometrics issuer and out of scope of this specification.

The Additional Biometrics EF creation mechanism is out of scope of this specification. Issuer SHOULD pre-create a number of Additional Biometrics EFs.

Note: Interindustry tags specified in the table below are used in LDS context, so coexistent tag allocation scheme is not required.

Table 93: EF.Biometrics Format

Tag	Tag	Content	MANDATORY/ OPTIONAL/ CONDITIONAL	Format	Example
7F2E		Biometric Data Template	M		'7F' '2E' Len {DO'5F2E' || DO'5F37' || DO'5F38'}
	5F2E	Additional Biometric data	M	V, B	'5F' '2E' Len {Biometric data}
	5F37	Authenticity token (Signature)	M	V (140), B	'5F' '37' Len {Signature}
	5F38	Reference (record number) to Additional Biometrics Signer certificate in Certificates Store	M	F (1) B	'01' …'40'

Note: B = Binary data, F = fixed-length field, V = variable- length field.

The order of the data objects in EF is fixed.

Each Additional Biometrics EF MUST contain a digital signature (Authenticity Token) calculated over the DO'5F2E, including Tag and Length. Signature is generated by the Additional Biometrics Signer.

Additional Biometrics Signer certificate required to verify Additional Biometric's signature is stored in a separate EF.Certificates store located under the Additional Biometrics application DF.

Each Additional Biometrics EF MUST be written using UPDATE BINARY command.

Additional Biometrics EF MUST NOT be altered (updated) or erased. The maximum number of Additional Biometrics EFs is 64.

All possible Additional Biometrics EF names, identifiers and short identifiers are listed in Table 94.

Table 94: EF.Biometrics Identifiers

EF name	EF identifier	Short EF identifier	EF name	EF identifier	Short EF identifier
EF.Biometrics1	'0201'	N/A	EF.Biometrics33	'0221'	N/A
EF.Biometrics2	'0202'	N/A	EF.Biometrics34	'0222'	N/A
EF.Biometrics3	'0203'	N/A	EF.Biometrics35	'0223'	N/A
EF.Biometrics4	'0204'	N/A	EF.Biometrics36	'0224'	N/A
EF.Biometrics5	'0205'	N/A	EF.Biometrics37	'0225'	N/A
EF.Biometrics6	'0206'	N/A	EF.Biometrics38	'0226'	N/A
EF.Biometrics7	'0207'	N/A	EF.Biometrics39	'0227'	N/A
EF.Biometrics8	'0208'	N/A	EF.Biometrics40	'0228'	N/A
EF.Biometrics9	'0209'	N/A	EF.Biometrics41	'0229'	N/A
EF.Biometrics10	'020A'	N/A	EF.Biometrics42	'022A'	N/A
EF.Biometrics11	'020B'	N/A	EF.Biometrics43	'022B'	N/A
EF.Biometrics12	'020C'	N/A	EF.Biometrics44	'022C'	N/A
EF.Biometrics13	'020D'	N/A	EF.Biometrics45	'022D'	N/A
EF.Biometrics14	'020E'	N/A	EF.Biometrics46	'022E'	N/A
EF.Biometrics15	'020F'	N/A	EF.Biometrics47	'022F'	N/A
EF.Biometrics16	'0210'	N/A	EF.Biometrics48	'0230'	N/A
EF.Biometrics17	'0211'	N/A	EF.Biometrics49	'0231'	N/A
EF.Biometrics18	'0212'	N/A	EF.Biometrics50	'0232'	N/A
EF.Biometrics19	'0213'	N/A	EF.Biometrics51	'0233'	N/A
EF.Biometrics20	'0214'	N/A	EF.Biometrics52	'0234'	N/A
EF.Biometrics21	'0215'	N/A	EF.Biometrics53	'0235'	N/A
EF.Biometrics22	'0216'	N/A	EF.Biometrics54	'0236'	N/A
EF.Biometrics23	'0217'	N/A	EF.Biometrics55	'0237'	N/A
EF.Biometrics24	'0218'	N/A	EF.Biometrics56	'0238'	N/A
EF.Biometrics25	'0219'	N/A	EF.Biometrics57	'0239'	N/A
EF.Biometrics26	'021A'	N/A	EF.Biometrics58	'023A'	N/A
EF.Biometrics27	'021B'	N/A	EF.Biometrics59	'023B'	N/A
EF.Biometrics28	'021C'	N/A	EF.Biometrics60	'023C'	N/A
EF.Biometrics29	'021D'	N/A	EF.Biometrics61	'023D'	N/A
EF.Biometrics30	'021E'	N/A	EF.Biometrics62	'023E'	N/A
EF.Biometrics31	'021F'	N/A	EF.Biometrics63	'023F'	N/A
EF.Biometrics32	'0220'	N/A	EF.Biometrics64	'0240'	N/A

5.4 LDS2 Application File Access Conditions (CONDITIONAL)

5.4.1 Roles and Default Authorization Levels (MANDATORY)

Each CV certificate contains a Certificate Holder Authorization Template (CHAT) that identifies the certificate holder role (IS, DV, CVCA) and contains access rights to DG3/DG4 of the REQUIRED LDS2 eMRTD Application (for legacy reasons or other national uses).

CHAT comprises a sequence of 2 objects:

1. An object identifier specifying the terminal type and the format of the template [TR- 03110]:
   id-roles OBJECT IDENTIFIER ::= {bsi-de applications(3) mrtd(1) 2}
   id-IS OBJECT IDENTIFIER ::= {id-roles 1}
2. A discretionary data object (tag '53') containing bit-encoded role and read-only access rights of the certificate holder according to the following table:

Table 95: Default CHAT Authorization

	Description	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Role	CVCA	1	1						
	DV (domestic)	1	0						
	DV (foreign)	0	1						
	IS	0	0						
Read Access	RFU								
	RFU								
	RFU								
	RFU								
	DG4 (Iris)							1	
	DG3 (Finger)								1

Note: The LDS2 eMRTD MUST ignore the value of RFU bits in the Certificate Holder Authorization.

5.4.2 Application Authorization Levels (MANDATORY)

Certificate holder authorizations for each LDS2 application are encoded in CV-certificate- extensions (one extension per application). Certificate extension is a discretionary template (tag ‘73’) comprising 2 data objects - an Authorization Object Identifier (tag ‘06’) for a specific application and a discretionary data object (tag ‘53’) containing bit-encoded access rights of the certificate holder to specified application.

To determine the effective authorization of a certificate holder, the LDS2 eMRTD chip calculates a bitwise Boolean ’and’ of the access rights contained in the certificate extensions of the IS Certificate and referenced DV and CVCA Certificates.

For Travel Records application the Authorization Object Identifiers and access right encoding are:

id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 3}

Table 96: Authorizations for Travel Records Application

	Description	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Access rights	RFU								
	RFU								
	RFU								
	RFU								
	Append EF.Certificates					1			
	Read/Search/Select/FMM EF.Certificates						1		
	Append EF.EntryRecords/ExitRecords							1	
	Read/Search/Select/FMM EF.EntryRecords/ExitRecords								1

For Visa Records application the Authorization Object Identifiers and access right encoding are:

```
id-icao-lds2-visaRecords          OBJECT IDENTIFIER     ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-access   OBJECT IDENTIFIER     ::= {id-icao-lds2-visaRecords 3}
```

Table 97: Authorizations for Visa Records Application

	Description	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Access rights	RFU								
	RFU								
	RFU								
	RFU								
	Append EF.Certificates					1			
	Read/Search/Select/FMM EF.Certificates						1		
	Append EF.VisaRecords							1	
	Read/Search/Select/FMM EF.VisaRecords								1

For Additional Biometrics application the Authorization Object Identifiers and access right encoding are:

```
id-icao-lds2-additionalBiometrics          OBJECT IDENTIFIER ::= {id-icao-lds2 3}
id-icao-lds2-additionalBiometrics-access OBJECT IDENTIFIER::= {id-icao-lds2-additionalBiometrics 3}
```

Table 98: Authorizations for Additional Biometrics Application

	Description	EF identifier	Authorizations							
			b8	b7	b6	b5	b4	b3	b2	b1
Byte 1	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	Append EF.Certificates	011A							1	
	Select/FMM/Read/Search EF.Certificates	011A								1
Byte 2	Select/FMM/Write/Activate/Read EF.Biometrics1 in Deactivated state	0201	1							
	Select/FMM/Read EF.Biometrics1 in Activated state	0201		1						
	Select/FMM/Write/Activate/Read EF.Biometrics2 in Deactivated state	0202			1					
	Select/FMM/Read EF.Biometrics2 in Activated state	0202				1				
	Select/FMM/Write/Activate/Read EF.Biometrics3 in Deactivated state	0203					1			
	Select/FMM/Read EF.Biometrics3 in Activated state	0203						1		
	Select/FMM/Write/Activate/Read EF.Biometrics4 in Deactivated state	0204							1	
	Select/FMM/Read EF.Biometrics4 in Activated state	0204								1
	...									
Byte 17	Select/FMM/Write/Activate/Read EF.Biometrics61 in Deactivated state	023D	1							
	Select/FMM/Read EF.Biometrics61 in Activated state	023D		1						
	Select/FMM/Write/Activate/Read EF.Biometrics62 in Deactivated state	023E			1					
	Select/FMM/Read EF.Biometrics62 in Activated state	023E				1				
	Select/FMM/Write/Activate/Read EF.Biometrics63 in Deactivated state	023F					1			
	Select/FMM/Read EF.Biometrics63 in Activated state	023F							1	
	Select/FMM/Write/Activate/Read EF.Biometrics64 in Deactivated state	0240								1
	Select/FMM/Read EF.Biometrics64 in Activated state	0240								1

Note1: The LDS2 eMRTD MUST ignore the value of RFU bits in the Certificate Holder Authorization.

Note2: Issuing State or organization MUST NOT issue terminal certificates with Write/Activate authorizations to the IS that are only supposed to read Additional Biometrics and not supposed to write them.

6 OBJECT IDENTIFIERS

6.1 LDS1 and LDS2 Application Object Identifiers Summary

Table 99: LDS1.7, LDS1.8 and LDS2 OIDs

Object Identifier	Value	Comments
id-icao	joint-iso-itu-t(2) international-organizations(23) icao(136)	ICAO OID
id-icao-mrtd	id-icao 1	eMRTD OID
id-icao-mrtd-security	id-icao-mrtd 1	
id-icao-ldsSecurityObject	id-icao-mrtd-security 1	LDS security object
id-icao-mrtd-security-cscaMasterList	id-icao-mrtd-security 2	CSCA master list
id-icao-mrtd-security-cscaMasterListSigningKey	id-icao-mrtd-security 3	
id-icao-mrtd-security-documentTypeList	id-icao-mrtd-security 4	document type list
id-icao-mrtd-security-aaProtocolObject	id-icao-mrtd-security 5	Active Authentication protocol
id-icao-mrtd-security-extensions	id-icao-mrtd-security 6	CSCA name change
id-icao-mrtd-security-extensions-nameChange	id-icao-mrtd-security-extensions 1	
id-icao-mrtd-security-extensions-documentTypeList	id-icao-mrtd-security-extensions 2	DS document type
id-icao-mrtd-security-DeviationList	id-icao-mrtd-security 7	Defect List Base OIDs
id-icao-mrtd-security-DeviationListSigningKey	id-icao-mrtd-security 8	
id-icao-lds2	id-icao-mrtd-security 9	LDS2 Object Identifiers
id-icao-lds2-travelRecords	id-icao-lds2 1	Travel Records application base OID
id-icao-lds2-travelRecords-application	id-icao-lds2-travelRecords 1	Travel Records AID
id-icao-lds2-travelRecords-access	id-icao-lds2-travelRecords 3	Authorization certificate extension
id-icao-lds2-visaRecords	id-icao-lds2 2	Visa Records application base OID
id-icao-lds2-visaRecords-application	id-icao-lds2-visaRecords 1	Visa Records AID
id-icao-lds2-visaRecords-access	id-icao-lds2-visaRecords 3	Authorization certificate extension
id-icao-lds2-additionalBiometrics	id-icao-lds2 3	Additional Biometrics base OID
id-icao-lds2-additionalBiometrics-application	id-icao-lds2-additionalBiometrics 1	Additional Biometrics AID
id-icao-lds2-additionalBiometrics-access	id-icao-lds2-additionalBiometrics 3	Authorization certificate extension
id-icao-lds2Signer	id-icao-lds2 8	LDS2 Signers Object Identifiers
id-icao-tsSigner	id-icao-lds2Signer 1	LDS2 Travel Stamp Signer certificate
id-icao-vSigner	id-icao-lds2Signer 2	LDS2 Visa Signer certificate
id-icao-bSigner	id-icao-lds2Signer 3	LDS2 Biometrics Signer certificate
id-icao-spoc	id-icao-mrtd-security 10	SPOC Object Identifiers
id-icao-spocClient	id-icao-spoc 1	Client
id-icao-spocServer	id-icao-spoc 2	Server

7 ASN.1 SPECIFICATIONS

id-icao OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) international-organizations(23) icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 2}
id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 3}
id-icao-mrtd-security-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 4}
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 5}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-mrtd-security-extensions 1}
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-security-extensions 2}
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 8}

id-icao-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

-- LDS2 Travel Records application Object Identifiers
id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 3}

-- LDS2 Visa Records application Object Identifiers
id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 1}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 3}

-- LDS2 Additional Biometrics application Object Identifiers
id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}
id-icao-lds2-additionalBiometrics-application OBJECT IDENTIFIER ::= {id-icao-lds2-additionalBiometrics 1}
id-icao-lds2-additionalBiometrics-access OBJECT IDENTIFIER ::= {id-icao-lds2-additionalBiometrics 3}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-lds2 8}
id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}
id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}
id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}
id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}
id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}

8 REFERENCES (NORMATIVE)

ISO/IEC 14443-1	ISO/IEC 14443-1:2018, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics*
ISO/IEC 14443-2	ISO/IEC 14443-2:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface*
ISO/IEC 14443-3	ISO/IEC 14443-3:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision*
ISO/IEC 14443-4	ISO/IEC 14443-4:2018, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*
ISO/IEC 10373-6	ISO/IEC 10373-6:2016, *Identification cards — Test methods — Part 6: Proximity cards*
ISO/IEC 18745-2	ISO/IEC 18745-2:2016 *Information technology — Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test methods for the contactless interface*
ISO/IEC 7816-2	ISO/IEC 7816-2:2007, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*
ISO/IEC 7816-4	ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*
ISO/IEC 7816-5	ISO/IEC 7816-5:2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*
ISO/IEC 7816-6	ISO/IEC 7816-6:2016, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange (Defect report included)*
ISO/IEC 7816-11	ISO/IEC 7816-11:2017, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*
ISO/IEC 8825-1	ISO/IEC 8825-1:2008, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*
ISO/IEC 19794-4	ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*
ISO/IEC 19794-5	ISO/IEC 19794-5:2005*, Information technology — Biometric data interchange formats — Part 5: Face image data*
ISO/IEC 19794-6	ISO/IEC 19794-6:2005*, Information technology — Biometric data interchange formats — Part 6: IRIS image data*
ISO/IEC 10646	ISO/IEC 10646:2012*, Information technology — Universal Coded Character Set (UCS)*
RFC 3369	Cryptographic Message Syntax 2002
ISO/IEC 10918-1	ISO/IEC 10918-1:1994, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*
ISO/IEC 15444	ISO/IEC 15444-n, *JPEG 2000 image coding system*
ISO/IEC 19785	ISO/IEC 19785-n, *Information technology — Common Biometric Exchange Formats Framework*
ISO/IEC 19795-6	ISO/IEC 19795-6:2012, *Information technology -- Biometric performance testing and reporting – Part 6: Testing methodologies for operational evaluation*
ISO/IEC 39794-4	ISO/IEC 39794-4, *Information technology — Extensible biometric data interchange formats — Part 4: Finger image data*
ISO/IEC 39794-5	ISO/IEC 39794-5, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*
ISO/IEC 39794-6	ISO/IEC 39794-6, *Information technology — Extensible biometric data interchange formats — Part 6: Iris image data*

APPENDIX A to Part 10 LOGICAL DATA STRUCTURE MAPPING EXAMPLES (INFORMATIVE)

The following informative text describes examples of mapping of the Logical Data Structure (LDS v1.7) using a random access representation to a contactless integrated circuit on an eMRTD.

A.1 EF.COM Common Data Elements

The following example indicates an implementation of LDS Version 1.7 using Unicode Version 4.0.0 having Data Groups 1 (tag '61'), 2 (tag '75'), 4 (tag '76'), and 12 (tag '6C') present.

For this and all other examples, the Tags are printed in **bold**, the Lengths printed *italics*, and the Values are printed in roman. Hexadecimal Tags, lengths and values are in quote marks ('xx').

'60' *'16'*
'5F01' *'04'* '0107'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

The example would read in full hexadecimal representation as:

'60' *'16'*
'5F01' *'04'* '30313037'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

A hypothetic LDS Version 15.99 would be encoded as:

'60' *'16'*
'5F01' *'04'* '1599'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

or hexadecimal:

'60' *'16'*
'5F01' *'04'* '31353939'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

A.2 EF.DG1 Machine Readable Zone Information

A.2.1TD1 Size eMRTD

An example of the DG1 using this information in a TD1 size LDS1 eMRTD is shown below. The length of the MRZ data element is 90 bytes (‘5A’).

‘61’ *‘5D’* **‘5F1F’** *‘5A’*

I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARIANNE<LOUISE

A.2.2 TD2 Size eMRTD

An example of the DG1 using this information in a TD2 size LDS1 eMRTD is shown below. The length of the MRZ data element is 72 bytes (‘48’).

‘61’ *‘4B’* **‘5F1F’** *‘48’*

I<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<54

A.3 EF.DG2 to EF.DG4 Biometric Templates

DG2 to DG4 use the nested off-card option of [ISO/IEC 7816-11] to have the possibility to store multiple biometric templates of a kind which are in harmony with the Common Biometric Exchange File Format (CBEFF), [NISTR 6529a]. The biometric sub-header defines the type of biometric that is present and the specific biometric feature.

Example: One signed, facial biometric with the biometric data block length of 12 642 bytes (‘3162’ bytes), encoded using a device with a PID of ‘00 01 00 01’, using format type ‘00 04’ owned by template provider ‘00 0A’ was captured on 15 March 2002 (no UTC offset) and is valid from 1 April 2002 through 31 March 2007. ICAO patron template Version 1.0 is being used.

The total length of the template is 12 704 bytes. The template is stored starting at the beginning of EF.DG2 (SFID 02).

‘75’ *‘82319EC’*
- **‘7F61’** *‘823199’*
  - **‘02’** *‘01’* ‘01’
  - **‘7F60’** *‘823191’*
  - **‘A1’** *‘26’*
    - **‘80’** *‘02’* ‘0101’
    - **‘81’** *‘01’* ‘02’
    - **‘83’** *‘07’* ‘20020315133000’
    - **‘85’** *‘08’* ‘2002040120070331’
    - **‘86’** *‘04’* ‘00010001’
    - **‘87’** *‘02’* ‘0101’
    - **‘88’** *‘02’* ‘0008’
  - **‘5F2E’** *‘823162’* ‘… 12 642 bytes of biometric data …’

A.4 EF.DG5 to EF.DG7 Displayed Image Templates

Note: One EF for each DG.
Example: Image template with the displayed image data length of 2 000 bytes. The length of the template is 2 008 bytes ('07D8').

'65' *'8207D8'*
'02' *'01'* 1
'5F40' *'8207D0'* '….2 000 bytes of image data …'

A.5 EF.DG11 Additional Personal Details

The following example shows the following personal details: Full name (John J. Smith), Place of birth (Anytown, MN), Permanent address (123 Maple Rd, Anytown, MN), Telephone number 1-612-555-1212 and Profession (Travel Agent). The length of the template is 99 bytes (*'63*').

'6B' *'63'*
'5C' *'0A'* **'5F0E' '5F11' '5F42' '5F12' '5F13'**
'5F0E' *'0D'* SMITH<<JOHN<J
'5F11' *'0A'* ANYTOWN<MN
'5F42' *'17'* 123 MAPLE RD<ANYTOWN<MN
'5F12' *'0E'* 16125551212
'5F13' *'0C'* TRAVEL<AGENT

A.6 EF.DG16 Person(s) To Notify

Example with two entries: Charles R. Smith of Anytown, MN and Mary J. Brown of Ocean Breeze, CA. The length of the template is 162 bytes ('A2').

'70' *'81A2'*
'02' *'01'* 2
'A1' '4C'
'5F50' *'08'* 20020101
'5F51' *'10'* SMITH<<CHARLES<R
'5F52' *'0B'* 19525551212
'5F53' *'1D'* 123 MAPLE RD<ANYTOWN<MN<55100
'A2' '4F'
'5F50' *'08'* 20020315
'5F51' *'0D'* BROWN<<MARY<J
'5F52' *'0B'* 14155551212
'5F53' *'23'* 49 REDWOOD LN<OCEAN BREEZE<CA<94000

— — — — — — — —

APPENDIX B to Part 10 THE CONTACLESS IC IN AN eMRP (INFORMATIVE)

B.1 The Antenna Size and Class of an eMRTD

The antenna size is at the discretion of the issuing State. With the exception of the antenna size, both the LDS1 and LDS2 eMRTD shall fulfil all tests specified in [ISO/IEC 18745-2] applying the Class 1 specifications.

It is RECOMMENDED for eMRTDs to be also compliant with Class 1 specifications.

There is no mandatory position of the IC, which MAY be placed in an arbitrary position. The location of the contactless antenna is at the discretion of the issuing State as long as it is in one of the following locations:

Data page — IC and antenna within the structure of a data page forming an internal page;
Centre of booklet — Placing the IC and its antenna between the centre pages of the book;
Cover — Placement within the structure or construction of the cover;
Separate sewn-in page — Incorporating the IC and its antenna into a separate page, which MAY be in the form of an ID3 size plastic card, sewn into the book during its manufacture; or
Back cover — Placement within the structure or construction of the back cover.

B.2 Booting and Polling

An eMRTD brought to an alternate magnetic field of 1.5 A/m as measured in [ISO/IEC 18745-2] shall respond to any REQ/WUP appropriate to its Type after an unmodulated alternate magnetic field of 10 ms. It is RECOMMENDED to be able to respond to any REQ/WUP appropriate to its Type after an unmodulated alternate magnetic field of 5 ms.

B.3 Anticollision and Type

The eMRTD MAY either declare compliance with Type A or with Type B as defined in [ISO/IEC 14443-2]. It shall not change its Type unless it has been reset by the eMRTD associated Inspection System.

B.4 Mandatory Bit Rates

The eMRTD shall provide at least the following bit rates, as defined in [ISO/IEC 14443-2], mandatorily: 106 kbit/s and 424 kbit/s in both directions between the eMRTD and the eMRTD associated Inspection System.

The bit rate of 212 kbit/s, and all bit rates from 848 kbit/s up to 6.78 Mbit/s for both directions, and from 10.17 Mbit/s to 27.12 Mbit/s from the eMRTD associated Inspection System to the eMRTD, as defined in [ISO/IEC 14443-2], are optional.

B.5 Electromagnetic Disturbance (EMD)

The support of EMD is not mandatory.

Note:The EMD feature enhances the robustness of the contactless communication between the eMRTD and the eMRTD associated Inspection System against eMRTD generated electromagnetic disturbance. The eMRTD dynamic current consumption during execution of a command may cause an arbitrary load modulation effect (which may not be purely resistive) on the magnetic field. In some cases, the eMRTD associated Inspection System may misinterpret EMD as data sent by the eMRTD, and this may negatively impact proper reception of the eMRTD response.

B.6 (Optional) Support of Exchange of Additional Parameters

The eMRTD MAY support the exchange of additional parameters as defined in [ISO/IEC 14443-4] in order to negotiate bit rates higher than 106 kbit/s. It MAY also use the same additional parameters to negotiate frames with error correction as specified in[ISO/IEC 14443-4].

B.7 Shielding

It is RECOMMENDED to not shield any page of the eMRTD.

B.8 (Recommended) Unique Identifier (UID) and Pseudo-unique PICC Identifier (PUPI)

The eMRTD MAY provide a random or fixed UID/PUPI as defined in [ISO/IEC 14443-3].

It is RECOMMENDED to use a random UID/PUPI to enhance the eMRTD holder's privacy and to reduce the possibility of tracking.

B.9 (Recommended) Resonance Frequency Range

There is no requirement on the resonance frequency of eMRTD. Applicants MAY limit the resonance frequency by default to a certain range to increase interoperability.

B.10 (Recommended) Frame Sizes

The eMRTD MAY support frame sizes of up to 4 kbyte according to [ISO/IEC 14443]. However, it is RECOMMENDED to support frame sizes of at least 1 kbyte. If supporting frame sizes higher than 1 kbyte, the use of frames with error correction as defined in [ISO/IEC 14443-4] is RECOMMENDED.

Note: A higher frame size substantially decreases the total processing time of an eMRTD application.

B.11 (Recommended) Frame Waiting Time Integer (FWI) and S-block Request for Waiting Time Extension [S(WTX)]

It is RECOMMENDED for the eMRTD to set an FWI value of less or equal to 11 in order to enhance performance. It is RECOMMENDED to use S(WTX) commands to extend the Frame Waiting Time for each particular command that requires additional time by using S(WTX) commands of an WTXM no greater than 10.

In case multiple S(WTX) requests are sent by the eMRTD, the total processing time for the current I-Block is RECOMMENDED to not exceed 5s.

Note: Lower FWI values as RECOMMENDED herein decrease the loss of time in transmission errors substantially, whereas S(WTX) are the ideal means of providing more time when needed.

APPENDIX C INSPECTION SYSTEMS (INFORMATIVE)

C.1 Operating Volume and Test Positions

An eMRTD associated Inspection System shall have an operating volume in accordance with one of the defined Inspection System types in [ISO/IEC 18745-2]. The operating volume is the volume in which all requirements of this technical report are fulfilled.

Note: The test positions for each Inspection System Type are further specified in [ISO/IEC 18745-2] with respect to the (device) 0 mm surface of the eMRTD associated Inspection System.

C.2 Particular Waveform and RF Requirements

The waveforms of the alternate magnetic field used to communicate shall be fully compliant with [ISO/IEC 14443-2]. In general, there are no exceptions or divergences from the basic standard, except for the field strength.

For eMRTD associated Inspection Systems of Type 1, 2 and 3, the field strength is RECOMMENDED to be at least 2 A/m at all positions for Class 1. For eMRTD associated Inspection Systems of Type M, the field strength shall be at least 1.5 A/m at all positions for Class 1.

Note: It may be desirable for eMRTDs to also communicate with other contactless Inspection Systems and mobile devices, e.g. NFC smartphones use 1.5 A/m.

C.3 Polling Sequences and eMRTD Detection Time

The polling sequence of the eMRTD associated Inspection System shall provide 10 ms of unmodulated carrier before any REQA/WUPA or REQB/WUPB.

For fast detection and processing, the eMRTD Inspection System:

- Shall poll for Type A and Type B with an equal occurrence of requests for both Types;
- for Inspection System Types 1, 2 and 3, one RF reset should occur in between any REQ/WUP of the same type;
- Shall guarantee at least one polling command for both Type A and Type B within 150 ms for an eMRTD present in the minimum mandatory operating volume according [ISO/IEC !8745- 2] at any position.

The eMRTD Inspection System MAY poll for contactless products of any other modulation type on the carrier of 13.56 MHz as long as all the requirements above are fulfilled.

Note:The unmodulated carrier of 10 ms is required to detect all eMRTDs in the field and is based on former specifications.

C.4 Mandatory Bit Rates

The eMRTD associated Inspection System shall provide mandatorily: 106 kbit/s and 424 kbit/s in both directions from the eMRTD to the eMRTD associated Inspection System and vice versa.

The bit rate of 212 kbit/s, and all bit rates from 848 kbit/s up to 6.78 Mbit/s for both directions and from 10.17 Mbit/s to 27.12 Mbit/s from eMRTD associated Inspection System to eMRTD as defined in [ISO/IEC 14443-2], are optional

C.5 Electromagnetic Disturbance (EMD)

The support of EMD is not mandatory.

Note: The EMD feature enhances the robustness of the contactless communication between the eMRTD and the eMRTD associated Inspection System against eMRTD generated electromagnetic disturbance. The eMRTD dynamic current consumption during execution of a command may cause an arbitrary load modulation effect (which may not be purely resistive) on the magnetic field. In some cases, the eMRTD associated Inspection System may misinterpret EMD as data sent by the eMRTD and this may

negatively impact proper reception of the eMRTD response.

C.6 Supported Antenna Classes

The eMRTD associated Inspection System of Type 1 and Type 2 shall at least support Class 1 eMRTDs in the operating volume. Class 2 and Class 3 are mandatory in ISO/IEC 14443, but optional for eMRTD Inspection System.

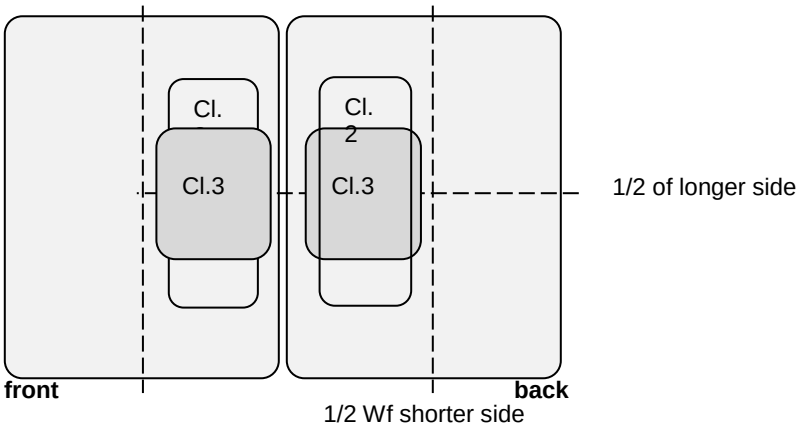


Figure C-1. Mandatory Positions in Each ID-3 Surface in which a Class 2 and Class 3 Antenna Shall be Read by an eMRTD Associated Inspection System of Type 1 and 2.

C.7 (Optional) Frame Sizes and Error Correction

The eMRTD associated Inspection System MAY optionally support all frame sizes of up to 4 kbyte as defined in [ISO/IEC 14443-3]. It is RECOMMENDED to use frames with error correction as defined in [ISO/IEC 14443-3] for all supported frame sizes higher than 1 kbyte.

Note: For eMRTD associated Inspection Systems of Type M, frame sizes higher than the 256 byte are currently not envisaged.

C.8 (Optional) Support of Additional Classes

eMRTD associated Inspection Systems of all Types MAY in addition support Class 4, Class 5 and Class 6 to be interoperable, for example, with mobile devices providing less coupling to the eMRTD associated Inspection System antenna coil.

C.9 (Recommended) Operating Temperature

It is RECOMMENDED that the eMRTD associated Inspection System works with temperatures of -10° to 50° Celsius.

C.10 (Recommended) Support of Multiple eMRTDs and other cards or objects or Multiple Hosts

It is highly RECOMMENDED to design the eMRTD associated Inspection System to handle more than one eMRTD, or one eMRTD and any other card or object compliant with [ISO/IEC 14443].

One of the following rules or a combination MAY be applied, among others:

- Apply full anticollision algorithms defined in [ISO/IEC 14443-3];
- Check for support of [ISO/IEC 14443-4] and dismiss all non-supporting cards;

- Check for an eMRTD application;
- Use CID and NAD.

Note: NAD may be also used for mobile devices with multiple hosts.

C.11 (Recommended) Frame Sizes

The eMRTD associated Inspection System MAY support frame sizes of up to 4 kbyte according to [ISO/IEC 14443-3]. However, it is RECOMMENDED to support frame sizes of at least 1 kbyte. If supporting frame sizes of 1 kbyte or higher, the use of frames with error correction as defined in [ISO/IEC 14443-4] is RECOMMENDED.

It is RECOMMENDED to perform any splitting of payload from the application layer into a minimum number of frames with an effective length of the maximum supported frame size with the exception of the last frame.

C.12 (Recommended) Error Recovery

Subsequent to a transmission error or an unresponsive eMRTD, it is RECOMMENDED for the eMRTD associated Inspection System to send a second R(NAK) according to the Inspection System rule 4 of [ISO/IEC 14443-4].

C.13 (Recommended) Error Detecting and Recovery Mechanism

When using the optional bit rates as well as optional frame sizes of higher than 256 byte, in case of a higher than usual number of transmission errors, it is RECOMMENDED to reduce the bit rate and effective frame size.

APPENDIX D Document Security Object EF.SOD VERSION V0 LDS v1.7 (LEGACY) (INFORMATIVE)

The Document Security Object V0 for the LDS v1.7 does not contain the LDS and Unicode version information:

```
LDSSecurityObject ::= SEQUENCE {
      version LDSSecurityObjectVersion,
      hashAlgorithm DigestAlgorithmIdentifier,
      dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
      DataGroupHash}
```

D.1 SignedData Type for SOD V0

The Document Security Object is implemented as a SignedData Type, as specified in [RFC 3369]. All security objects SHALL be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

Note 1: m MANDATORY — the field SHALL be present.
Note 2: x do not use — the field SHOULD NOT be populated.
Note 3: o optional — the field MAY be present.
Note 4: c choice — the field content is a choice from alternatives.

Signed Data Type for SO_D V0

Value		Comments
SignedData		
Version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject.
Certificates	o	States may choose to include the Document Signer Certificate (CDS) which can be used to verify the signature in the signerInfos field.
Crls	x	It is recommended that States do not use this field.
signerInfos	m	It is recommended that States provide only 1 signerInfo within this field.
SignerInfo	m	
Version	m	The value of this field is dictated by the sid field. See RFC3369 Doc 9303-12 for rules regarding this field.
Sid	m	
issuerandSerialNumber	c	It is recommended that States support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving States may choose to ignore them.

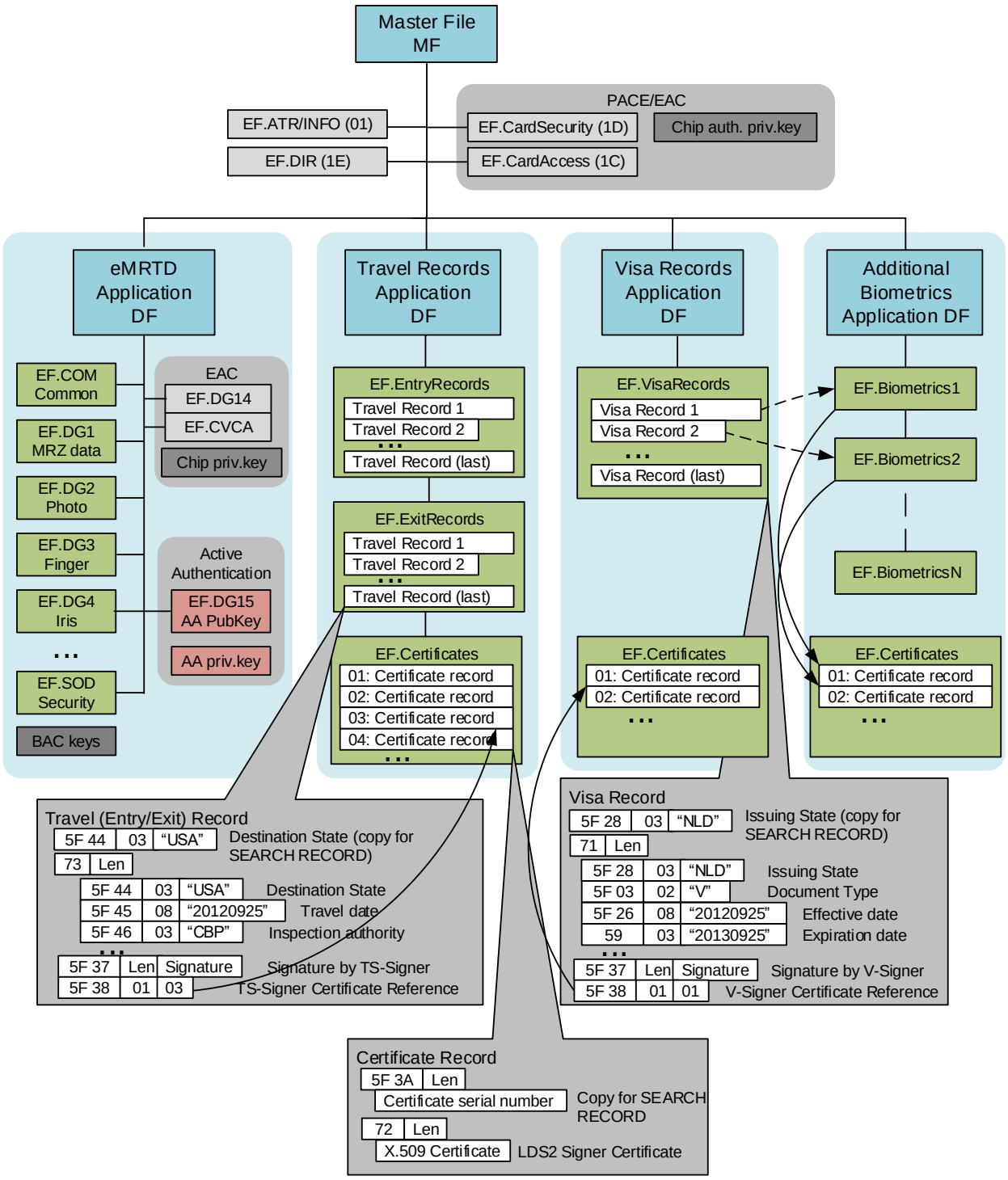
D.2 *ASN.1 Profile LDS Document Security Object for SOD VO*

```
LDSSecurityObjectV0 {joint-iso-itu-t (2) international(23) icao(136) mrtd(1) security(1)
ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

-- Imports from RFC 3280 [PROFILE],
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) };

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao   OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}
id-icao-mrtd  OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security     OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber         DataGroupNumber,
   dataGroupHashValue      OCTET STRING }
DataGroupNumber ::= INTEGER {
   dataGroup1               (1),
   dataGroup2               (2),
   dataGroup3               (3),
   dataGroup4               (4),
   dataGroup5               (5),
   dataGroup6               (6),
   dataGroup7               (7),
   dataGroup8               (8),
   dataGroup9               (9),
   dataGroup10             (10),
   dataGroup11             (11),
   dataGroup12             (12),
   dataGroup13             (13),
   dataGroup14             (14),
   dataGroup15             (15),
   dataGroup16             (16)}
END
```

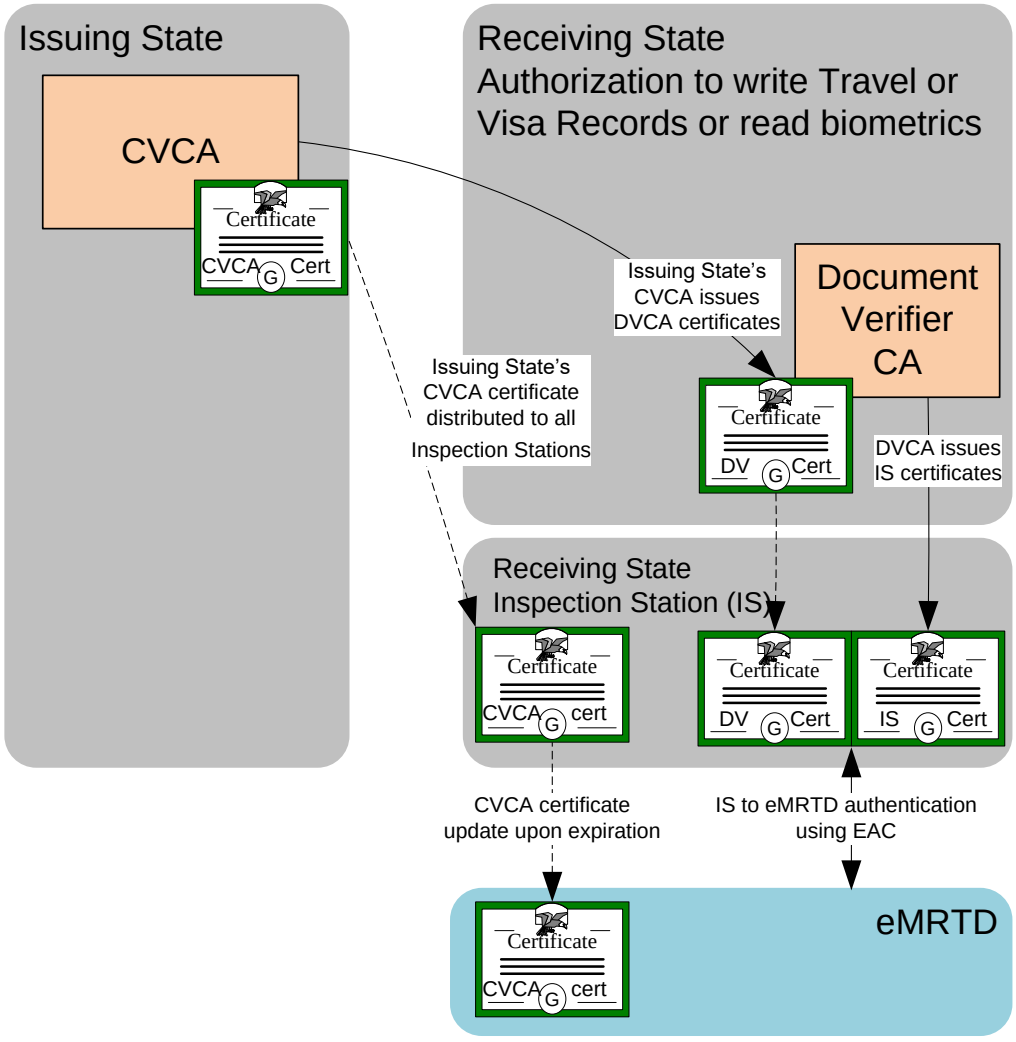
Note 1: The field `dataGroupHashValue` *contains the calculated hash over the complete contents of the Data Group EF, specified by* `dataGroupNumber`*.*

Note 2: `DigestAlgorithmIdentifiers` *MUST omit "*`NULL`*" parameters, while the* `SignatureAlgorithmIdentifier` *(as defined in RFC 3447) MUST include* `NULL` *as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754.* Inspection system MUST accept the field `DigestAlgorithmIdentifiers` with both conditions, i.e. absent parameters and `NULL` parameters.

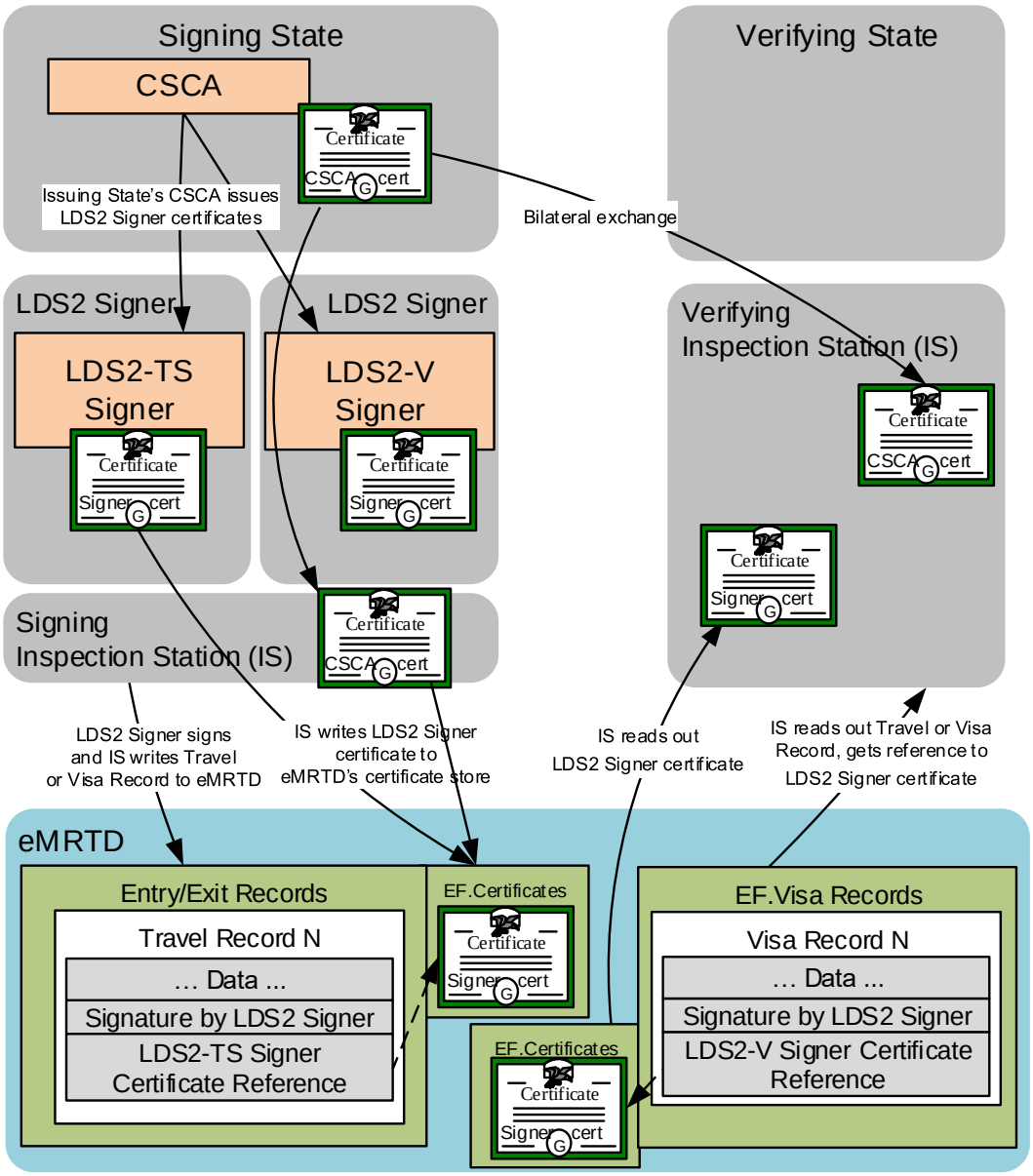
APPENDIX E FILE STRUCTURES SUMMARY
(INFORMATIVE)



APPENDIX F LDS AUTHORIZATION SUMMARY
(INFORMATIVE)



APPENDIX G LDS DIGITAL SIGNATURE SUMMARY
(INFORMATIVE)



APPENDIX H EXAMPLE READING TRAVEL RECORDS
(INFORMATIVE)

1) FMM command retrieving the number of Entry Records

CLA	INS	P1	P2	Lc	Data	Le
80	5E	01	04	04	51 02 01 01	00

CLA: Proprietary class / no secure messaging
INS: FMM
P1: 01 - EF identifier in command data field
P2: 04 - Return existing number of records in a record EF
Lc: 04
Data: DO'51 containing Entry Records EF identifier '0101'
Le : 00 (Short Le)

Response: FILE AND MEMORY MANAGEMENT DO representing the number of records in the EF

Data	SW1-SW2
7F78 03 83 01 FD	90 00

The DO in the response data contains the last record number which can be used in the next READ RECORD command (P1).

Ex., last record number '00' means that there are no records in this file, response 'FD' means that number of records is 253 (maximum number of records is 254).

2a) Read Record command retrieving the last Travel Record from the retrieved list

The following command can be used to retrieve a single record using record number returned by the FMM command:

CLA	INS	P1	P2	Le
00	B2	FD	04	00 00 00

CLA : Interindustry class / no secure messaging
INS : READ RECORD(S)
P1 : Record number from the previous command's response
P2 : Record number in P1 / read record P1
Le : 00 00 00 (Extended Le) - read entire record

Response: Record - 253 ('FD')

Data	SW1-SW2
5F44 Len <Data> || 73 Len <Data> || 5F37 Len <Data> || 5F38 Len <Data>	90 00

2b) READ RECORD retrieving last 2 Travel Records from the retrieved list

The following command can be used to retrieve 2 (or more) records from the list returned by FMM command. Reading several records in one APDU exchange improves performance. The number of records that can be retrieved by a single command can be determined from extended length information in EF.ATR/INFO and maximum size of Travel Record.

CLA	INS	P1	P2	Le
00	B2	FC	05	00 00 00

CLA : Interindustry class / no secure messaging

INS : READ RECORD(S)
P1 : Decremented Record number from the FMM response (253 - 1 = 252 = 'FC')
P2 : Record number in P1 / read all records from P1 up to the last
Le : 00 00 00 (Extended Le) - read entire record

Response: Last 2 records - 252 ('FC') and 253 ('FD')

Data	SW1-SW2
5F44 Len <Data> || 73 Len <Data> || 5F37 Len <Data> || 5F38 Len <Data> || 5F44 Len <Data> || 73 Len <Data> || 5F37 Len <Data> || 5F38 Len <Data>	90 00

APPENDIX I EXAMPLE SEARCHING RECORDS BY STATE
(INFORMATIVE)

SEARCH RECORD command searching Travel Record() by destination State

CLA	INS	P1	P2	Lc	Data	Le
00	A2	00	F8	Var	7F 76 Len 51 01 01 A1 0B 80 01 00 B0 06 02 01 03 02 01 03 A3 07 B1 05 81 03 xx xx xx	00

CLA: Interindustry class / no secure messaging
INS: SEARCH RECORD(S)
P1: record number = 00
P2: Search through multiple EFs
Lc: length of command data field
Data: DO'7F76' - Record handling DO
DO'51' - File reference DO (EF.EntryRecords short identifier '01')
DO'A1' - Search configuration template
DO'80' - Search configuration parameter: '00' (search all records)
DO'B0' - Search window template
DO'02' - Offset: '03'
DO'02' - Number of bytes: '03'
DO'A3' - Search string template
DO'B1' - Search string DO
DO'81' - Search string (country code): xx xx xx
Le: 00 (Short Le)

Response: DO'7F76' – Record handling DO
DO'51' - EF.EntryRecords short identifier '01'
One or more DO'02' containing matching record numbers

Data	SW1-SW2
7F 76 Len 51 01 01 02 01 03 02 01 04	90 00

APPENDIX K EXAMPLE WRITING TRAVEL RECORD AND CERTIFICATE
(INFORMATIVE)

SEARCH RECORD Command Searching EF.Certificates by a Certificate Serial Number

IS checks if LDS2-TS Signer certificate with required serial numbers exists in EF.Certificates. The following command can be used for searching certificates:

CLA	INS	P1	P2	Lc	Data	Le
00	A2	00	F8	Var	7F 76 Len 51 01 1A A1 0B 80 01 30 B0 06 02 01 03 02 01 {Search string size} A3 Len B1 Len 81 Len xx xx .. xx xx	00

CLA: Interindustry class / no secure messaging
INS: SEARCH RECORD(S)
P1: record number = 00
P2: Search through multiple EFs
Lc: length of command data field
Data: DO'7F76' - Record handling DO
DO'51' - File reference DO (EF.Certificates short identifier '1A')
DO'A1' - Search configuration template
DO'80' - Search configuration parameter: '30' (stop if record found)
DO'B0' - Search window template
DO'02' - Offset: '03'
DO'02' - Number of bytes: Search string size
DO'A3' - Search string template
DO'B1' - Search string DO
DO'81' - Search concatenation of country code and certificate serial number: xx xx .. xx xx
Le: 00 (Short Le)

Response: DO'7F76' - Record handling DO
DO'51' - EF.Certificates short identifier '1A'
DO'02' - contains matching record number

Data	SW1-SW2
7F 76 06 51 01 1A 02 01 **01**	90 00

or warning code 62 82 if no record matches the search criteria:

SW1-SW2
62 82

If an EF.Certificate record matches the search criteria, the IS can optionally use the returned record number (‘01’) in a READ RECORD command to check whether the certificate is the correct one. If no EF.Certificate record matches the search criteria, the IS writes the certificate into EF.Certificates using the APPEND RECORD command in step 2) and finally writes the entry record using step 3).

APPEND RECORD Command Writing Certificate

IS writes LDS2-TS Signer certificate into EF.Certificates. The following command can be used for writing certificates:

CLA	INS	P1	P2	Lc	Data	Le
00	E2	00	D0	00 XX XX	5F3A Len {certificate serial number} || 72 Len {X.509 certificate}”	Absent

CLA: Interindustry class / no secure messaging
INS: APPEND RECORD
P1: 00 (any other value is invalid)
P2: short EF identifier (=’1A’) Lc:
Record length (Extended Lc)
Data: Record data

Response: success or error code

SW1-SW2
90 00

APPEND RECORD Command Writing Travel Record

IS generates Travel Record using reference to LDS2-TS Signer certificate and writes it into EF.EntryRecords using the following command:

CLA	INS	P1	P2	Lc	Data	Le
00	E2	00	08	00 XX XX	5F44 Len {destination state} || 73 Len {Entry travel record} || 5F37 Len {Signature} || 5F38 Len {Cert Ref}	Absent

CLA: Interindustry class / no secure messaging
INS: APPEND RECORD
P1: 00 (any other value is invalid)
P2: short EF identifier (=’01’) Lc:
Record length (Extended Lc)
Data: Record data

Response: success or error code

SW1-SW2
90 00

----------END----------

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2020

Part 11: Security Mechanisms for MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 11 — *Security Mechanisms for MRTDs*
ISBN 978-92-9249-799-6

DOCUMENT CHANGE RECORD

Doc 9303, Part 11

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

Page

1. SCOPE

This Part 11 provides specifications to enable States and suppliers to implement cryptographic security features for electronic machine readable travel documents (“eMRTDs”) offering contactless integrated circuit (IC) access. Cryptographic protocols are specified to:

- prevent skimming of data from the contactless IC;
- prevent eavesdropping on the communication between contactless IC and reader;
- provide authentication of the data stored on the contactless IC based on the Public Key Infrastructure (PKI) described in Part 12; and
- provide authentication of the contactless IC itself.

The Eight Edition of Doc 9303 incorporates the specifications for the optional Travel Records, Visa Records, and Additional Biometrics applications (known as *LDS2 applications*) as an optional extension of the eMRTD. This part of Doc 9303 includes the necessary extended access control protocols to protect writing and reading of the data of the respective LDS2 applications. These access control protocols may also be used for the protection of the secondary biometrics in the eMRTD Application.

The authentication of the data stored on the contactless IC is the basic security feature to enable the use of the IC for manual and/or automated inspection. This feature is therefore REQUIRED.

Implementation of a protocol to prevent skimming of the data stored on the contactless IC and to prevent eavesdropping on the communication between IC and terminal is REQUIRED.

Implementation of the other protocols is OPTIONAL, allowing the issuing State or organization to decide on the necessary set of security features according to national regulations/demands.

This Part shall be read in conjunction with the following Parts of Doc 9303:

- Part 1 — *Introduction*;
- Part 10 — *Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*; and
- Part 12 — *Public Key Infrastructure for MRTDs*.

2. ASSUMPTIONS AND NOTATIONS

It is assumed that the reader of this document is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

Whilst the use of public key cryptography techniques adds some complexity to the implementation of eMRTDs, such techniques add value in that they will provide front-line border control points with an additional measure to determine the authenticity of the eMRTD. It is assumed that the use of such a technique is not the sole measure for determining authenticity and it SHOULD NOT be relied upon as a single determining factor.

In the event that the data from the contactless IC cannot be used, for instance as a result of a certificate revocation or an invalid signature verification, or if the contactless IC was left intentionally blank (see section 4.5.4 of Doc 9303-10), the eMRTD is not necessarily invalidated. In such cases a receiving State MAY rely on other document security features for validation purposes.

2.1 Requirements for eMRTD Chips and Terminals

This Part of Doc 9303 specifies requirements for implementations of eMRTD chips (or, equivalently, IC) and terminals (or inspection systems). While eMRTD chips must comply with those requirements according to the terminology described in Doc 9303-1, requirements for terminals are to be interpreted as guidance, i.e. interoperability of eMRTD chip and terminal are only guaranteed if the terminal complies with those requirements, otherwise the interaction with the eMRTD chip will either fail or the behaviour of the eMRTD chip is undefined. In general, the eMRTD chip need not enforce requirements related to terminals unless the security of the eMRTD chip is directly affected.

2.2 Notations

The following notations are used to denote cryptographic primitives in an algorithm independent way:

- Encryption of clear text *S* with symmetric key *K*: **E***(K, S)*;
- Decryption of cipher text *C* with symmetric key *K*: **D***(K, C)*;
- The operation for computing a hash over a message *m* is denoted by **H***(m)*.
- Computing a Message Authentication Code with symmetric key *K* over message *M*: **MAC***(K ,M)*;
- Key agreement based on asymmetric key pairs *(SK, PK)* and *(SK', PK')* and domain parameters *D*: **KA***(SK,PK',D)* / **KA***(SK',PK,D)*;
- Key derivation from a shared secret *S*: **KDF***(S)*;
- Signing a message *m* with private key SK_{IFD} is denoted by *s* = **Sign***(SK_{IFD}, m)*;
- Verifying the resulting signature *s* with public key PK_{IFD} and message *m*: **Verify***(PK_{IFD}, s, m)*.
- Computing a compressed representation of a public key *PK*: **Comp***(PK)*.

3. SECURING ELECTRONIC DATA

Besides Passive Authentication by digital signatures and Chip Access Control, issuing States or organizations MAY choose additional security, using more complex ways of securing the contactless IC and its data.

Accessing an eMRTD comprises the following steps:

1. Gain access to the contactless IC of the eMRTD (Section 4)
2. Authentication of data (Section 5)

3. Authentication of the chip (Section 6)
4. Additional access control mechanisms (Section 7)
5. Reading data (see Doc 9303-10).

Different protocols are available for the different steps. The exact configuration of an eMRTD is chosen by the issuing State or organization. The options given in Table 1 can be suitably combined to achieve additional security according to the requirements of issuers.

Inspection Procedures for different configurations of eMRTDs are described in Appendix J.

Table 1. Securing Electronic Data (Summary)

Method	***Contactless IC***	***Inspection System***	***Benefits***	***Note***
BASELINE SECURITY METHOD				
Passive Authentication (Section 5.1)	m	m	Proves that the contents of the SO_D and the LDS are authentic and not changed.	Does not prevent an exact copy or IC substitution. Does not prevent unauthorized access. Does not prevent skimming.
ADVANCED SECURITY METHODS				
Comparison of conventional MRZ(OCR-B) and IC-based MRZ(LDS)	n/a	o	Proves that contactless IC's content and physical eMRTD belong together.	Adds (minor) complexity. Does not prevent an exact copy of contactless IC and conventional document.
Active Authentication (Section 6.1)	o	o	Prevents copying the SO_D and proves that it has been read from the authentic contactless IC. Proves that the contactless IC has not been substituted.	Does not prevent unauthorized access. Adds complexity. Chip Authentication is REQUIRED for LDS2.
Chip Authentication (Section 6.2)	o / c	o		

Method	*Contactless IC*	*Inspection System*	*Benefits*	*Note*
Basic Access Control (BAC) (Section 4.3)	c (see also 4.1)	m (see also 4.1)	Prevents skimming and misuse. Prevents eavesdropping on the communications between eMRTD and inspection system (when used to set up encrypted session channel).	Does not prevent an exact copy or IC substitution (requires also copying of the conventional document). Adds complexity. At least one of BAC or PACE SHALL be supported by the eMRTD. PACE is REQUIRED for LDS2. PACE offers better protection against eavesdropping than BAC. See also Appendix A
Password Authenticated Connection Establishment (PACE) (Section 4.4)	r / c (see also 4.1)	m (see also 4.1)		
Terminal Authentication (Section 7.1)	o / c	o	Prevents unauthorized access to sensitive data. Prevents skimming of sensitive data.	Requires additional key management. Does not prevent an exact copy or IC substitution (requires also copying of the conventional document). Adds complexity. Terminal Authentication is REQUIRED for LDS2.
Data Encryption (Section 7.2)	o	o	Secures additional biometrics. Does not require processor-ICs.	Requires complex decryption key management. Does not prevent an exact copy or IC substitution. Adds complexity.
m = REQUIRED, r = RECOMMENDED, o = OPTIONAL, c = CONDITIONAL, n/a = not applicable.				

Note.— See Section 4 for details on compliant configurations of contactless ICs with respect to the implementation of Basic Access Control and Password Authenticated Connection Establishment.

Implementation of advanced security methods as listed in Table 1 does not affect ICAO compliance.

4. ACCESS TO THE CONTACTLESS IC

Adding a contactless IC without access control to an eMRTD introduces two new attack possibilities:

- the data stored in the contactless IC can be electronically read without authorizing this reading of the document (skimming); and
- the unencrypted communication between a contactless IC and a reader can be eavesdropped within a

distance of several metres.

While there are physical measures possible against skimming (e.g. shielding using a metal mesh in the cover of a passport booklet), these do not address eavesdropping. Therefore, it is understood that issuing States or organizations SHALL implement a Chip Access Control mechanism, i.e. an access control mechanism that in effect requires the knowledge of the bearer of the eMRTD that the data stored in the contactless IC is being read in a secure way. This Chip Access Control mechanism prevents skimming as well as eavesdropping.
A contactless IC that is protected by a Chip Access Control mechanism denies access to its contents unless the inspection system can prove that it is authorized to access the contactless IC. This proof is given in a cryptographic protocol, where the inspection system proves knowledge of the information derived from the physical document.

The inspection system MUST be provided with this information prior to being able to read the contactless IC. The information has to be retrieved optically/visually from the eMRTD (e.g. from the MRZ). It also MUST be possible for an inspector to enter this information manually in the inspection system in case machine-reading of the information is not possible.

Assuming that the information from the physical document cannot be obtained from an unviewed document (e.g. since the information is derived from the optically read MRZ), it is accepted that the eMRTD was knowingly handed over for inspection. Due to the encryption of the channel, eavesdropping on the communication would require a considerable effort.

This section defines two mechanisms for Chip Access Control:

- Basic Access Control (BAC, Section 4.3), which is based purely on symmetric cryptography; and
- Password Authenticated Connection Establishment (PACE, Section 4.4), which employs asymmetric cryptography to provide higher entropy session keys.

See also Appendix A for additional information on the strength of session keys.

4.1 Compliant Configurations

The following configurations comply with this specification:

- eMRTD chips implementing BAC only;
- eMRTD chips implementing PACE *and* BAC;
- Starting 1 January 2018, eMRTD chips implementing PACE only.

Note. — BAC may become deprecated in the future. In this case PACE will become the default access control mechanism.

Compliant inspection systems MUST support all compliant eMRTD configurations. If an eMRTD supports both PACE and BAC, the inspection system SHALL use either BAC or PACE but not both in the same session.

Note.— Previous versions of Doc 9303 allowed eMRTD chips implementing no Chip Access Control ("plain eMRTDs"). This is deprecated in the 8th edition. Nevertheless, compliant inspection systems MUST support eMRTDs without Chip Access Control.

Note.— For access to LDS2 applications, the IC MUST require the execution of PACE.

4.2 Chip Access Procedure

The chip access procedure to authenticate the inspection system consists of the following steps.

1. **Read EF.CardAccess** **(REQUIRED)**

   If PACE is supported by the eMRTD, the eMRTD chip MUST provide the parameters to be used for PACE in the file EF.CardAccess.

   If EF.CardAccess is available, the inspection system SHALL read the file EF.CardAccess (cf. Section 9.2.11) to determine the parameters (i.e. symmetric ciphers, key agreement algorithms, domain parameters, and mappings) supported by the eMRTD chip. The inspection system may select any of those parameters.

   If the file EF.CardAccess is not available or does not contain parameters for PACE, the inspection system SHOULD try to read the eMRTD with Basic Access Control (skip to Step 4).

2. Read EF.DIR **(OPTIONAL)**

   The Inspection System MAY read EF.DIR (if present) to retrieve a list of applications present on the eMRTD chip.

3. **PACE** **(CONDITIONAL)**

   This step is RECOMMENDED if PACE is supported by the eMRTD chip. This step is REQUIRED if access to LDS2 applications is intended.

   - The inspection system SHOULD derive the key K_π from the MRZ. It MAY use the CAN instead of the MRZ if the CAN is known to the inspection system.
   - The eMRTD chip SHALL accept the MRZ as passwords for PACE. It MAY additionally accept the CAN instead of the MRZ.
   - The inspection system and the eMRTD chip mutually authenticate using K_π and derive session keys KS_{Enc} and KS_{MAC}. The PACE protocol as described in Section 4.4 SHALL be used.

   If successful, the eMRTD chip performs the following:

   - It SHALL start Secure Messaging.
   - It SHALL grant access to less sensitive data (e.g. EF.DG1, EF.DG2, EF.DG14, EF.DG15, etc. of the eMRTD Application, and the Document Security Object — for the definition of “sensitive data” see Doc 9303-1).
   - It SHALL restrict access rights to require Secure Messaging.

   The inspection system MUST verify the authenticity of the contents of EF.CardAccess using EF.DG14 or EF. CardSecurity, and of EF.DIR (if present and read) using EF.CardSecurity.

   Note: If no LDS2 application is present on the eMRTD chip, EF.CardSecurity may not contain a secured copy of EF.DIR.

4. **Basic Access Control** **(CONDITIONAL)**

This step is REQUIRED if Chip Access Control is enforced by the eMRTD chip and PACE has not been used. If PACE was successfully performed or if the eMRTD does not enforce Chip Access Control, this step is skipped.

The eMRTD Application MUST be selected before Basic Access Control is performed.

- The inspection system SHOULD derive the Document Basic Access Keys (K_{Enc} and K_{MAC}) from the MRZ.
- The inspection system and the eMRTD chip mutually authenticate using the Document Basic Access Keys and derive session keys KS_{Enc} and KS_{MAC}.

If successful, the eMRTD chip performs the following:

- It SHALL start Secure Messaging.
- It SHALL grant access to less sensitive data (e.g. EF.DG1, EF.DG2, EF.DG14, EF.DG15, etc. of the eMRTD Application, and the Document Security Object).
- It SHALL restrict access rights to require Secure Messaging.

Note.— As a result of the Chip Access Procedure, the Current DF can be either the Master File (if PACE was used) or the eMRTD Application (if BAC was used).

4.3 Basic Access Control

4.3.1 Protocol Specification

Authentication and Key Establishment is provided by a three-pass challenge-response protocol according to [ISO/IEC 11770-2] Key Establishment Mechanism 6 using 3DES [FIPS 46-3] as block cipher. A cryptographic checksum according to [ISO/IEC 9797-1] MAC Algorithm 3 is calculated over and appended to the ciphertexts. The modes of operation described in Section 4.3.3 MUST be used. Exchanged nonces MUST be of size 8 bytes, exchanged keying material MUST be of size 16 bytes. The IFD (i.e. the inspection system) and the contactless IC MUST NOT use distinguishing identifiers as nonces.

In more detail, IFD and IC SHALL perform the following steps:

1) The IFD requests a challenge RND.IC by sending the GET CHALLENGE command. The IC generates and responds with a nonce RND.IC.

2) The IFD performs the following operations:

   a) generate a nonce RND.IFD and keying material K.IFD.

   b) generate the concatenation S = RND.IFD || RND.IC || K.IFD.

   c) compute the cryptogram E_{IFD} = **E**($K_{Enc,}$ S).

d) compute the checksum M_{IFD} = **MAC**(K_{MAC}, E_{IFD}).

e) send the EXTERNAL AUTHENTICATE command with mutual authenticate function using the data E_{IFD} || M_{IFD}.

3) The IC performs the following operations:

a) check the checksum M_{IFD} of the cryptogram E_{IFD}.

b) decrypt the cryptogram E_{IFD}.

c) extract RND.IC from S and check if IFD returned the correct value.

d) generate keying material K.IC.

e) generate the concatenation R = RND.IC || RND.IFD || K.IC.

f) compute the cryptogram E_{IC} = **E**(K_{Enc}, R).

g) compute the checksum M_{IC} = **MAC**(K_{MAC}, E_{IC}).

h) send the response using the data E_{IC} || M_{IC}.

4) The IFD performs the following operations:

a) check the checksum M_{IC} of the cryptogram E_{IC}.

b) decrypt the cryptogram E_{IC}.

c) extract RND.IFD from R and check if IC returned the correct value.

5) The IFD and the IC derive session keys KS_{Enc} and KS_{MAC} using the key derivation mechanism described in Section 9.7.1. / 9.7.4 with (K.IC xor K.IFD) as shared secret.

4.3.2 Inspection Process

When an eMRTD with Basic Access Control is offered to the inspection system, optically or visually read information is used to derive the Document Basic Access Keys (K_{Enc} and K_{MAC}) to gain access to the contactless IC and to set up a secure channel for communications between the eMRTD's contactless IC and the inspection system.

An eMRTD's contactless IC that supports Basic Access Control MUST respond to unauthenticated read attempts, i.e. read attempts sent without Secure Messaging (including selection of (protected) files in the LDS), with "Security status not satisfied" (0x6982) once the Secure Channel is established. If the IC receives a plain SELECT, i.e. without Secure Messaging applied, in the Secure Channel, the IC SHALL abort the Secure Channel. When a plain SELECT is sent before the Secure Channel is established, or when the Secure Channel has been aborted, both 0x6982 and 0x9000 MAY be returned by the IC, i.e., are ICAO-compliant responses.

To authenticate the inspection system the following steps MUST be performed:

1) The inspection system reads the "MRZ_information". The "MRZ_information" consists of the

concatenation of Document Number, Date of Birth and Date of Expiry, including their respective check digits, as described in Doc 9303-4, Doc 9303-5 or Doc 9303-6 for document form factors TD3, TD1 and TD2, respectively, from the MRZ using an OCR-B reader. Alternatively, the required information can be typed in; in this case it SHALL be typed in as it appears in the MRZ. The most significant 16 bytes of the SHA-1 hash of this "MRZ_information" are used as key seed to derive the Document Basic Access Keys using the key derivation mechanism described in Section 9.7.2.

2) The inspection system and the eMRTD's contactless IC mutually authenticate and derive session keys. The authentication and key establishment protocol described above MUST be used.

3) After a successful execution of the authentication protocol both the IFD and the IC compute session keys KS_{Enc} and KS_{MAC} using the key derivation mechanism described in Section 9.7.1 / 9.7.4 with (K.IC xor K.IFD) as shared secret. All subsequent communication MUST be protected by Secure Messaging as described in Section 9.8.

4.3.3 Cryptographic Specifications

4.3.3.1 Encryption of Challenge and Response

Two key 3DES in CBC mode with zero IV (i.e. 0x00 00 00 00 00 00 00 00) according to [ISO/IEC 11568-2] SHALL be used for computation of E_{IFD} and E_{IC}. Padding for the input data MUST NOT be used when performing the EXTERNAL AUTHENTICATE command.

4.3.3.2 Authentication of Challenge and Response

The cryptographic checksums M_{IFD} and M_{IC} SHALL be calculated using [ISO/IEC 9797-1] MAC algorithm 3 with block cipher DES, zero IV (8 bytes), and [ISO/IEC 9797-1] padding method 2. The MAC length MUST be 8 bytes.

4.3.4 Application Protocol Data Units

Basic Access Control is performed using the commands GET CHALLENGE and EXTERNAL AUTHENTICATE with mutual authenticate function. The commands SHALL be encoded as specified in [ISO/IEC 7816-4].

4.3.4.1 GET CHALLENGE

Command		
CLA		Context specific
INS	0x84	GET CHALLENGE
P1/P2	0x0000	—
Data		*Absent*
Response		

Data	Random Nonce	
Status Bytes	0x9000	*Normal processing* Random Nonce successfully generated and transmitted.
	Other	*Operating system dependent error* Random Nonce could not be transmitted.

4.3.4.2 EXTERNAL AUTHENTICATE

Command			
CLA		Context specific	
INS	0x82	EXTERNAL AUTHENTICATE	
P1/P2	0x0000	—	
Data		Command data E_{IFD} || M_{IFD}	REQUIRED
Response			
Data		Response data E_{IC} || M_{IC}	REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol has been performed successfully.	
	Other	*Operating system dependent error* The protocol failed.	

4.4 Password Authenticated Connection Establishment

PACE is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the eMRTD chip and the inspection system (i.e. eMRTD chip and inspection system share the same password π).

PACE establishes Secure Messaging between an eMRTD chip and an inspection system based on weak (short) passwords. The security context is established in the Master File. The protocol enables the eMRTD chip to verify that the inspection system is authorized to access stored data and has the following features:

- Strong session keys are provided independent of the strength of the password.
- The entropy of the password(s) used to authenticate the inspection system can be very low (e.g. 6 digits are sufficient in general).

PACE uses keys K_{π} derived from passwords with a key derivation function $\mathbf{KDF_{\pi}}$ (cf. Section 9.7.3). For globally interoperable machine readable travel documents the following two passwords and corresponding keys are available:

- MRZ: The key K_{π} defined by $K_{\pi} = \mathbf{KDF_{\pi}}$(MRZ) is REQUIRED. It is derived from the Machine Readable

Zone (MRZ) similar to Basic Access Control, i.e. the key is derived from the Document Number, the Date of Birth and the Date of Expiry.

- CAN: The key K_π defined by K_π = $\mathbf{KDF}_\pi$(CAN) is OPTIONAL. It is derived from the Card Access Number (CAN). The CAN is a number printed on the document and MUST be chosen randomly or pseudo-randomly (e.g. using a cryptographically strong pseudo-random function). Doc 9303 part 4, 5, and 6 specify the CAN field.

Note.— In contrast to the MRZ (Document Number, Date of Birth, Data of Expiry) the CAN has the advantage that it can easily be typed in manually.

PACE supports different Mappings as part of the protocol execution:

- *Generic Mapping* based on a Diffie-Hellman Key Agreement;
- *Integrated Mapping* based on a direct mapping of a field element to the cryptographic group;
- *Chip Authentication Mapping* extends the Generic Mapping and integrates Chip Authentication into the PACE protocol.

If the chip supports Chip Authentication Mapping, at least one of Generic Mapping or Integrated Mapping and Chip Authentication MUST also be supported by the chip. This implies that for inspection systems supporting PACE, only support for Generic Mapping and Integrated Mapping is REQUIRED. Support for Chip Authentication Mapping is OPTIONAL.

4.4.1 Protocol Specification

The inspection system reads the parameters for PACE supported by the eMRTD chip from the file EF.CardAccess (cf. Section 9.2.11) and selects the parameters to be used, followed by the protocol execution.

The following commands SHALL be used:

- READ BINARY as specified in Doc 9303-10;
- MSE:Set AT (MANAGE SECURITY ENVIRONMENT command with Set Authentication Template function) as specified in Section 4.4.4.1;
- The following steps SHALL be performed by the inspection system and the eMRTD chip using a chain of GENERAL AUTHENTICATE commands as specified in Section 4.4.4.2:

  1) The eMRTD chip randomly and uniformly chooses a nonce s, encrypts the nonce to z = $\mathbf{E}(K_\pi,s)$, where K_π = $\mathbf{KDF}_\pi$ (π) is derived from the shared password π, and sends the ciphertext z to the inspection system.

  2) The inspection system recovers the plaintext s = $\mathbf{D}(K_\pi,z)$ with the help of the shared password π.

  3) Both the eMRTD chip and the inspection system perform the following steps:

     a) They exchange additional data required for the mapping of the nonce:

        i) for the generic mapping, the eMRTD chip and the inspection system exchange ephemeral key

public keys.

ii) for the integrated mapping, the inspection system sends an additional nonce to the eMRTD chip.

b) They compute the ephemeral domain parameters D = **Map**(D_{IC},s,…) as described in Section 4.4.3.3.

c) They perform an anonymous Diffie-Hellman key agreement (cf. Section 9.6) based on the ephemeral domain parameters and generate the shared secret K = **KA**($SK_{DH,IC}$, $PK_{DH,IFD}$,D) = **KA**($SK_{DH,IFD}$,$PK_{DH,IC}$,D).

d) During Diffie-Hellman key agreement, the IC and the inspection system SHOULD check that the two public keys $PK_{DH,IC}$ and $PK_{DH,IFD}$ differ.

e) They derive session keys KS_{MAC} = $\mathbf{KDF}_{MAC}(K)$ and KS_{Enc} = $\mathbf{KDF}_{Enc}(K)$ as described in Section 9.7.1.

f) They exchange and verify the authentication token T_{IFD} = **MAC**(KS_{MAC},$PK_{DH,IC}$) and T_{IC} = **MAC**(KS_{MAC},$PK_{DH,IFD}$) as described in Section 4.4.3.4.

4) Conditionally, the eMRTD chip computes Chip Authentication Data CA_{IC}, encrypts them A_{IC} = **E**(KS_{Enc}, CA_{IC}) and sends them to the terminal (cf. Section 4.4.3.5.1). The terminal decrypts A_{IC} and verifies the authenticity of the chip using the recovered Chip Authentication Data CA_{IC} (cf. Section 4.4.3.5.2).

A simplified version of the protocol is also shown in Figure 1.

Chip denoted as IC		***Inspection system denoted as IFD***
Static domain parameters D_{IC} Choose random nonce s Compute z = **E**(K_π,s)		
	— z →	
		Compute s = **D**(K_π,z)
	← additional data for **Map** →	
D = **Map**(D_{IC},s,…) Choose random ephemeral key pair ($SK_{DH,IC}$, $PK_{DH,IC}$,D)		D = **Map**(D_{IC},s,…) Choose random ephemeral key pair ($SK_{DH,IFD}$,$PK_{DH,IFD}$,D)
	← $PK_{DH,IC}$, $PK_{DH,IFD}$ →	
Check $PK_{DH,IC} \neq PK_{DH,IFD}$ K = **KA**($SK_{DH,IC}$, $PK_{DH,IFD}$,D) Compute T_{IC} = **MAC**(KS_{MAC},$PK_{DH,IFD}$) [compute CA_{IC} and encrypt as A_{IC} = **E**(KS_{Enc}, CA_{IC}).]		Check $PK_{DH,IC} \neq PK_{DH,IFD}$ K = **KA**($SK_{DH,IFD}$,$PK_{DH,IC}$,D) Compute T_{IFD} = **MAC**(KS_{MAC},$PK_{DH,IC}$)
	← T_{IC}, T_{IFD} → [— A_{IC} →]	
Verify T_{IFD}		Verify T_{IC} [decrypt A_{IC} and authenticate chip]

Figure 1. Password Authenticated Connection Establishment

4.4.2 Security Status

An eMRTD chip that supports PACE SHALL respond to unauthenticated read attempts (including selection of (protected) files in the LDS) with “Security status not satisfied” (0x6982).

Note.— This specification is more restrictive than the corresponding specification for BAC-only eMRTDs.

If PACE was successfully performed then the eMRTD chip has verified the used password. Secure Messaging is started using the derived session keys KS_{MAC} and KS_{Enc}.

4.4.3 Cryptographic Specifications

This section contains the cryptographic details of the specification.

Particular algorithms are selected by the issuing State or organization. The inspection system MUST support all combinations described in the following subsections, with the exception of Chip Authentication Mapping, which is OPTIONAL. The eMRTD chip MAY support more than one combination of algorithms.

Note.— Some algorithms are not available for the Chip Authentication Mapping: For security reasons, the use of 3DES is no longer recommended. DH-variants are not available to reduce the number of variants to be implemented by Terminals.

4.4.3.1 DH

For PACE with DH the respective algorithms and formats from Section 9.6 and Table 2 MUST be used.

Table 2. Algorithms and Formats for DH

OID	***Mapping***	***Sym. Cipher***	***Key-length***	***Secure Messaging***	***Auth. Token***
id-PACE-DH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-DH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-DH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-DH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC

4.4.3.2 ECDH

For PACE with ECDH the respective algorithms and formats from Section 9.6 and Table 3 MUST be used.

Only prime curves with uncompressed points SHALL be used. The standardized domain parameters described in Section 9.5.1 SHOULD be used.

Table 3. Algorithms and Formats for ECDH

OID	***Mapping***	***Sym. Cipher***	***Key-length***	***Secure Messaging***	***Auth. Token***
id-PACE-ECDH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-ECDH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC
id-PACE-ECDH-CAM-AES-CBC-CMAC-128	Chip Authenti-cation	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-CAM-AES-CBC-CMAC-192		AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-CAM-AES-CBC-CMAC-256		AES	256	CBC / CMAC	CMAC

4.4.3.3 Encrypting and Mapping Nonces

The eMRTD chip SHALL randomly and uniformly select the nonce *s* as a binary bit string of length *l*, where *l* is a multiple of the block size in bits of the respective block cipher **E**() chosen by the eMRTD chip.

- The nonce s SHALL be encrypted in CBC mode according to [ISO/IEC 10116] using the key $K_\pi = KDF_\pi(\pi)$ derived from the password π and IV set to the all-0 string.
- The nonce s SHALL be converted to a random generator using an algorithm-specific mapping function **Map**.
- For the Integrated Mapping the additional nonce *t* SHALL be selected randomly and uniformly as a binary bit string of length *k* and sent in clear. In this case *k* is the key size in bits of the respective block cipher **E**() and *l* SHALL be the smallest multiple of the block size of **E**() such that $l \geq k$.

To map the nonce *s* or the nonces *s*, *t* into the cryptographic group one of the following mappings SHALL be used:

- *Generic Mapping* (Section 4.4.3.3.1);

- *Integrated Mapping* (Section 4.4.3.3.2);
- *Chip Authentication Mapping* (Section 4.4.3.3.3).

4.4.3.3.1 Generic Mapping

ECDH

The function **Map**:G → Ĝ is defined as Ĝ = s×G+H, where H in <G> is chosen such that $\log_G H$ is unknown. The point H SHALL be calculated by an anonymous Diffie-Hellman Key Agreement [TR-03111] as H = **KA**$(SK_{Map,IC}, PK_{Map,IFD}, D_{IC})$ = **KA**$(SK_{Map,IFD}, PK_{Map,IC}, D_{IC})$.

Note.— The key agreement algorithm ECKA prevents small subgroup attacks by using compatible cofactor multiplication.

DH

The function **Map**:g → ĝ is defined as ĝ =g^s×h, where h in <g> is chosen such that $\log_g h$ is unknown. The group element h SHALL be calculated by an anonymous Diffie-Hellman Key Agreement as h = **KA**$(SK_{Map,IC}, PK_{Map,IFD}, D_{IC})$ = **KA**$(SK_{Map,IFD}, PK_{Map,IC}, D_{IC})$.

Note.— The public key validation method described in [RFC 2631] MUST be used to prevent small subgroup attacks.

4.4.3.3.2 Integrated Mapping

ECDH

The function **Map**:G → Ĝ is defined as Ĝ = f_G(**R**$_p$(s,t)), where **R**$_p$() is a pseudo-random function that maps octet strings to elements of GF(p) and f_G() is a function that maps elements of GF(p) to <G>. The random nonce t SHALL be chosen randomly by the inspection system and sent to the eMRTD chip. The pseudo-random function **R**$_p$()is described below. The function f_G() is defined in [BCIMRT2010]. An informative description is given in Appendix B.

DH

The function **Map**:g → ĝ is defined as ĝ = f_g(**R**$_p$(s,t)), where **R**$_p$() is a pseudo-random function that maps octet strings to elements of GF(p) and f_g() is a function that maps elements of GF(p) to <g>. The random nonce t SHALL be chosen randomly by the inspection system and sent to the eMRTD chip. The pseudo-random function **R**$_p$() is described below. The function f_g() is defined as $f_g(x)=x^a \bmod p$, and a = (p-1)/q is the cofactor. Implementations MUST check that ĝ ≠ 1.

Pseudo-random Number Mapping

The function **R**$_p$(s,t) is a function that maps octet strings s (of bit length l) and t (of bit length k) to an element $\text{int}(x_1||x_2||...||x_n) \bmod p$ of GF(p). The function **R**$_p$(s,t) is specified below in Figure 2.

The construction is based on the respective block cipher **E**() in CBC mode according to [ISO/IEC 10116] with IV=0, where k is the key size (in bits) of **E**(). Where required, the output k_i MUST be truncated to key size k. The value n SHALL be selected as smallest number, such that $n*l \geq \log_2 p + 64$.

Note.— The truncation is only necessary for AES-192: Use octets 1 to 24 of k_i; additional octets are not used. In case of DES, k is considered to be equal to 128 bits, and the output of R(s,t) shall be 128 bits.

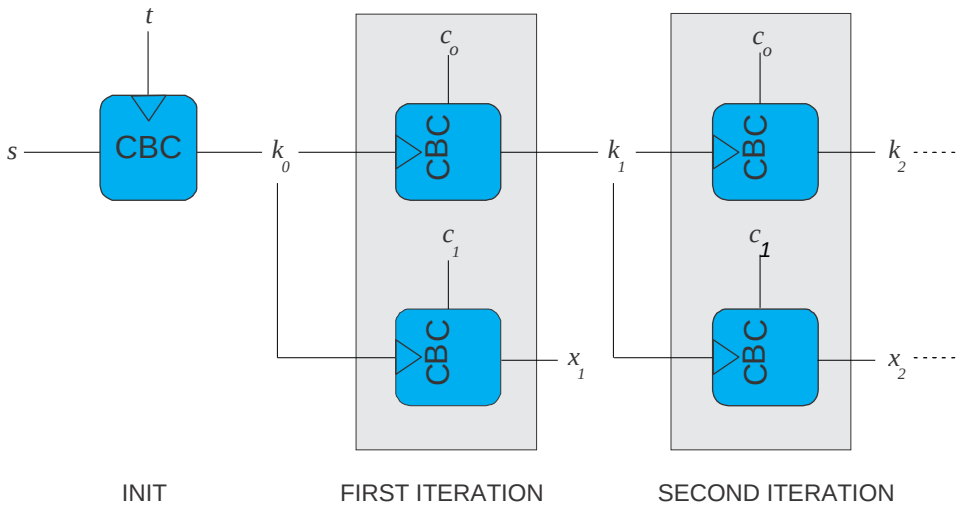


Figure 2. Pseudo-random number mapping

The constants c_0 and c_1 are defined as follows:

- For 3DES and AES-128 (l=128):
  - `c0=0xa668892a7c41e3ca739f40b057d85904`
  - `c1=0xa4e136ac725f738b01c1f60217c188ad`
- For AES-192 and AES-256 (l=256):
  - `c0= 0xd463d65234124ef7897054986dca0a174e28df758cbaa03f240616414d5a1676`
  - `c1= 0x54bd7255f0aaf831bec3423fcf39d69b6cbf066677d0faae5aadd99df8e53517`

4.4.3.3.3 Chip Authentication Mapping

The mapping phase of the PACE-CAM is identical to the mapping phase of PACE-GM (cf. Section 4.4.3.3.1).

4.4.3.4 Authentication Token

The authentication token SHALL be computed over a public key data object (cf. Section 9.4) containing the object identifier as indicated in MSE:Set AT (cf. Section 4.4.4.1), and the received ephemeral public key (i.e. excluding the domain parameters, cf. Section 9.4.4) using an authentication code and the key KS_{MAC} derived from the key agreement.

Note.— Padding is performed internally by the message authentication code, i.e. no application specific

padding is performed.

3DES

3DES [FIPS 46-3] SHALL be used in Retail-mode according to [ISO/IEC 9797-1] MAC algorithm 3 / padding method 2 with block cipher DES and IV=0.

AES

AES [FIPS 197] SHALL be used in CMAC-mode [SP 800-38B] with a MAC length of 8 bytes.

4.4.3.5 Encrypted Chip Authentication Data

The eMRTD chip MUST provide static key pair(s) SK_{IC}, PK_{IC} as described in Section 6.2. Encrypted Chip Authentication Data is REQUIRED for PACE with Chip Authentication Mapping.

4.4.3.5.1 Generation by the eMRTD chip

The Chip Authentication Data SHALL be computed as $CA_{IC} = (SK_{IC})^{-1} * SK_{Map,IC} \bmod p$, where SK_{IC} is the static private key of the chip, $SK_{Map,IC}$ is the ephemeral private key used by the chip to computer H in the mapping phase of PACE (cf. Section 4.4.3.3.1) and p is the order of the used cryptographic group. The Chip Authentication Data SHALL be encrypted using the key KS_{Enc} derived from the key agreement as A_{IC} = **E**(KS_{Enc}, CA_{IC}) to yield the Encrypted Chip Authentication Data.

Note.— $(SK_{IC})^{-1}$*can be precomputed during personalization of the eMRTD chip and securely stored in the chip, avoiding the modular inversion during run-time.*

4.4.3.5.2 Verification by the terminal

The terminal SHALL decrypt A_{IC} to recover CA_{IC} and verify $PK_{Map,IC}$ = **KA**$(CA_{IC}, PK_{IC}, D_{IC})$, where PK_{IC} is the static public key of the eMRTD chip.

Note.— Passive Authentication MUST be performed in combination with the Chip Authentication Mapping. Only after a successful validation of the respective Security Object may the eMRTD chip be considered genuine.

4.4.3.5.3 Padding

The data to be encrypted SHALL be padded according to [ISO/IEC 9797-1] “Padding Method 2”.

4.4.3.5.4 AES

AES [19] SHALL be used in CBC-mode according to [ISO/IEC 10116] with $IV=E(KS_{Enc},-1)$, where *-1* is the bit string of length 128 with all bits set to 1.

4.4.4 Application Protocol Data Units

The following sequence of commands SHALL be used to implement PACE:

1. MSE:Set AT
2. GENERAL AUTHENTICATE

4.4.4.1 MSE:Set AT

The command MSE:Set AT is used to select and initialize the PACE protocol. The use of MSE:Set AT for PACE is indicated by a PACE Object Identifier (see section 4.4.3 and 9.2.3) contained as cryptographic mechanism reference with tag 0x80, see below.

Command			
CLA		Context specific	
INS	0x22	Manage Security Environment	
P1/P2	0xC1A4	Set Authentication Template for mutual authentication	
Data	0x80	*Cryptographic mechanism reference* Object Identifier of the protocol to select (value only, Tag 0x06 is omitted).	REQUIRED
	0x83	*Reference of a public key / secret key* The password to be used is indicated by the following values in this data object: 0x01: MRZ_information 0x02: CAN	REQUIRED
	0x84	*Reference of a private key / Reference for computing a session key* This data object is REQUIRED to indicate the identifier of the domain parameters to be used if the domain parameters are ambiguous, i.e. more than one set of domain parameters is available for PACE.	CONDITIONAL
	0x7F4C	*Certificate Holder Authorization Template* This data object (defined in Doc 9303-12) MUST be present if the terminal requests Certification Authority Reference(s) for use in Terminal Authentication to be returned as part of PACE (cf. Section 4.4.5). The Object Identifier contained in this data object SHALL be set to `id-IS` (cf. Doc 9303-10). The access bits in the discretionary data template SHALL all be set to 1 by the terminal.	CONDITIONAL

Response		
Data	–	Absent
Status Bytes	0x9000	*Normal processing* The protocol has been selected and initialized.
	0x6A80	*Incorrect parameters in the command data field* Algorithm not supported or initialization failed.

	0x6A88	*Referenced data not found* The referenced data (i.e. password or domain parameter) is not available.
	other	*Operating system dependent error* The initialization of the protocol failed.

Note.— Some operating systems accept the selection of an unavailable key and return an error only when the key is used for the selected purpose.

Note.— For the MSE:Set command, the IC SHOULD ignore data objects with tags not specified for this command. The terminal SHOULD NOT include data objects with tags not known to be understood by the IC.

4.4.4.2 GENERAL AUTHENTICATE

A chain of GENERAL AUTHENTICATE commands is used to perform the PACE protocol.

Command			
CLA		Context specific.	
INS	0x86	GENERAL AUTHENTICATE	
P1/P2	0x0000	Keys and protocol implicitly known	
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects	REQUIRED
Response			
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects as described in Section 4.4.5.	REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol (step) was successful.	
	0x6300	*Authentication failed* The protocol (step) failed.	
	0x6A80	*Incorrect parameters in command data field* Provided data is invalid.	
	other	*Operating system dependent error* The protocol (step) failed.	

4.4.4.3 Command Chaining

Command chaining MUST be used for the GENERAL AUTHENTICATE command to link the sequence of commands to the execution of the protocol. Command chaining MUST NOT be used for other purposes unless clearly indicated by the chip. For details on command chaining see [ISO/IEC 7816-4].

4.4.5 Exchanged Data

The protocol specific data objects SHALL be exchanged in a chain of GENERAL AUTHENTICATE commands, with protocol specific command and response data encapsulated in a Dynamic Authentication data object (see Section 4.4.4.2) with context specific tags as shown in Table 4:

Table 4. Exchanged data for PACE

Step	***Description***	***Protocol Command Data***		***Protocol Response Data***	
1.	Encrypted Nonce	-	Absent[1]	0x80	Encrypted Nonce
2.	Map Nonce	0x81	Mapping Data	0x82	Mapping Data
3.	Perform Key Agreement	0x83	Ephemeral Public Key	0x84	Ephemeral Public Key
4.	Mutual Authentication	0x85	Authentication Token	0x86	Authentication Token
				0x87	Certification Authority Reference (CONDITIONAL)
				0x88	Certification Authority Reference (CONDITIONAL)
				0x8A	Encrypted Chip Authentication Data (CONDITIONAL)

Certification Authority Reference(s) MUST be present if a data object 0x7F4C was transmitted to the IC during set up of PACE (cf. Section 4.4.4.1) and Terminal Authentication is supported by the IC. In this case the data object 0x87 SHALL contain the most recent Certification Authority Reference. The data object 0x88 MAY contain the previous Certification Authority Reference.

Encrypted Chip Authentication Data (cf. Section 4.4.3.5) MUST be present if Chip Authentication Mapping is used and MUST NOT be present otherwise.

4.4.5.1 Encrypted Nonce

The encrypted nonce (cf. Section 4.4.3.3) SHALL be encoded as octet string.

4.4.5.2 Mapping Data

The exchanged data is specific to the used mapping:

4.4.5.2.1 Generic Mapping

1. This implies an empty Dynamic Authentication Data Object

The ephemeral public keys (cf. Section 4.4.3.3 and Section 9.4.4) SHALL be encoded as elliptic curve point (ECDH) or unsigned integer (DH).

4.4.5.2.2 Integrated Mapping

The nonce *t* SHALL be encoded as octet string.

Note.— The context specific data object 0x82 SHALL be empty for the Integrated Mapping.

4.4.5.2.3 Chip Authentication Mapping

The encoding of the mapping data is identical to the Generic Mapping (cf. Section 4.4.5.2.1).

4.4.5.3 Public Keys

The public keys SHALL be encoded as described in Section 9.4.4.

4.4.5.4 Authentication Token

The authentication token (cf. Section 4.4.3.4) SHALL be encoded as octet string.

4.4.5.5 Certification Authority Reference

The Certification Authority Reference (CAR) data objects SHALL be encoded as specified in Doc 9303-12.

4.4.5.6 Encrypted Chip Authentication Data

The Chip Authentication Data SHALL be encoded as octet string using the function FE2OS() specified in [TR-03111] before encryption. Note that FE2OS() requires the encoding with the same number of octets as the prime order of the group, i.e. possibly including leading 0x00's. The Encrypted Chip Authentication Data SHALL be encoded as octet string.

5. AUTHENTICATION OF DATA

In addition to the LDS Data Groups, the contactless IC also contains a Document Security Object (SO_D). This object is digitally signed by the issuing State or organization and contains hash representations of the LDS contents (see Doc 9303-10).

An inspection system, containing the Document Signer Public Key of each State, or having read the Document Signer Certificate (C_{DS}) from the eMRTD, will be able to verify the Document Security Object (SO_D). In this way, through the contents of the Document Security Object (SO_D), the contents of the LDS are authenticated.

This verification mechanism does not require processing capabilities of the contactless IC in the eMRTD. Therefore it is called “Passive Authentication” of the contactless IC’s contents.

Passive Authentication proves that the contents of the Document Security Object (SO_D) and LDS are authentic and not

changed. It does not prevent exact copying of the contactless IC's content or chip substitution.

Therefore Passive Authentication SHOULD be supported by an additional physical inspection of the eMRTD.

5.1 Passive Authentication

5.1.1 Inspection Process

The inspection system performs the following steps:

1. The inspection system SHALL read the Document Security Object (SO_D) (which MUST contain the Document Signer Certificate (C_{DS}), see also Doc 9303-10) from the contactless IC.

2. The inspection system SHALL build and validate a certification path from a Trust Anchor to the Document Signer Certificate used to sign the Document Security Object (SO_D) according to Doc 9303-12.

3. The inspection system SHALL use the verified Document Signer Public Key to verify the signature of the Document Security Object (SO_D).

4. The inspection system MAY read relevant Data Groups from the contactless IC.

5. The inspection system SHALL ensure that the contents of the Data Group are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SO_D).

The following additional checks are considered Best Practice:

1. The inspection system or the inspection officer SHOULD check the presence of a DocumentTypeExtension in the Document Signer Certificate.

   - If yes, the inspection system SHOULD check the consistency of the DocumentTypeExtension, the Document Type from Data Group 1 and the Document Type from the visual MRZ (see Docs 9303-12, 9303-10 and 9303-3, respectively).

   - If no, the inspection system SHOULD check that the KeyUsage of the Document Signer Certificate is set to digitalSignature and that the Document Signer Certificate contains no ExtendedKeyUsage-Extension (see Doc 9303-12).

2. The inspection system or the inspection officer SHOULD check the consistency of the country codes from:

   - the Subject-field and, if present, the SubjectAltName of the Document Signer Certificate;

   - the Subject-field and, if present, the SubjectAltName of the Trust Anchor (CSCA certificate);

   - the Data Group 1 as read from the contactless IC; and

   - the visual MRZ.

   Additionally, the inspection system or the inspection officer MAY compare the contents of Data Group 1 to the visual MRZ (see Docs 9303-12, 9303-10 and 9303-3, respectively).

3. The inspection system SHOULD verify that the Issuing Date of the eMRTD is included in the Private Key Usage Period contained in the Document Signer Certificate (see Doc 9303-12).

The biometric information can now be used to perform the biometrics verification with the person who offers the eMRTD.

5.1.2 Additional Inspection Process for LDS2 Applications

Data written after issuance of the eMRTD are not protected by the Document Security Object, which is signed by the issuer of the document. To verify the authenticity of data written after issuance, the following steps MUST be performed by the inspection system for each written data object:

1. The inspection system SHALL build and validate a certification path from a Trust Anchor to the Signer Certificate used to sign the data object according to Doc 9303-12. The inspection system MAY use both certificates known beforehand and certificates retrieved from the chip to build the path (see Doc 9303-10).

2. The inspection system SHALL use the verified Signer Public Key to verify the signature of the data object.

Note.—— This procedure can be skipped for data objects whose authenticity is not deemed relevant for the inspection process by the receiving State or organization.

6. AUTHENTICATION OF THE CONTACTLESS IC

An issuing State or organization MAY choose to protect its eMRTDs against chip substitution.

The following mechanisms to verify the authenticity of the chip are available.

1. *Active Authentication*, as defined in Section 6.1. Support of Active Authentication is indicated by the presence of EF.DG15. If available, the terminal MAY read and verify EF.DG15 and perform Active Authentication.

2. *Chip Authentication*, as defined in Section 6.2. Support of Chip Authentication is indicated by the presence of corresponding `SecurityInfos` in EF.DG14/EF.CardSecurity. If available, the terminal MAY read and verify EF.DG14/EF.CardSecurity and perform Chip Authentication.

3. *PACE with Chip Authentication Mapping* (PACE-CAM) as defined in Section 4.4. Support is indicated by the presence of a corresponding `PACEInfo` structure in EF.CardAccess. If PACE-CAM was performed successfully in the chip access procedure, the terminal MAY perform the following to authenticate the chip:

   - read and verify EF.CardSecurity

   - use the Public Key from EF.CardSecurity together with the Mapping Data and the Chip Authentication Data received as part of PACE-CAM to authenticate the chip (Section 4.4.3.5.2).

6.1 Active Authentication

Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC.

For this purpose the contactless IC contains its own Active Authentication Key pair (KPr_{AA} and KPu_{AA}). A hash

representation of Data Group 15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPr_{AA}) is stored in the contactless IC's secure memory.

By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SO_D)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPr_{AA} and KPu_{AA}), the inspection system verifies that the Document Security Object (SO_D) has been read from the genuine contactless IC, stored in the genuine eMRTD.

Active Authentication requires processing capabilities of the eMRTD's contactless IC.

6.1.1 Protocol Specification

Active Authentication is performed using the [ISO/IEC 7816-4] INTERNAL AUTHENTICATE command.

If Active Authentication is performed after Secure Messaging was established, all commands and responses MUST be transmitted as Secure Messaging APDUs according to Section 9.8.

In more detail, IFD (inspection system) and IC (eMRTD's contactless IC) perform the following steps:

1. The IFD generates a nonce RND.IFD and sends it to the IC using the INTERNAL AUTHENTICATE command.

2. The IC performs the following operations:

   a) generate the message M;

   b) calculate h(M);

   c) compute the signature σ and send the response to the IFD.

3. The IFD verifies the response on the sent INTERNAL AUTHENTICATE command and checks if the IC returned the correct value.

6.1.2 Cryptographic Specifications

6.1.2.1 Nonce

The input is a nonce (RND.IFD) that MUST be 8 bytes.

Note.— Nonces MUST NOT be reused, e.g. the nonce used for BAC/PACE MUST NOT be reused for Active Authentication.

6.1.2.2 RSA

The IC SHALL compute a signature, when an integer factorization based mechanism is used, according to [ISO/IEC 9796-2] Digital Signature scheme 1.

In the following, k denotes the length of key for signature generation and L_h the length of the output of the hash function H used during signature generation. The trailer field option 1 MUST be used (and t set to 1) if SHA-1 is used during signature generation, trailer field option 2 MUST be used otherwise (and t set to 2).

The following values for the trailer field SHALL be used for option 2:

Hash function	SHA-224	SHA-256	SHA-384	SHA-512
Trailer field	0x38CC	0x34CC	0x36CC	0x35CC

For interoperability reasons, only SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 are supported as hash functions for Active Authentication with RSA.

The message M to be signed SHALL be the concatenation of M1 and M2, where M1 MUST be a nonce of length c - 4 bits (RND.IC) generated by the eMRTD, where c (the *capacity of the signature*) is given by $c = k - L_h - (8 \times t) - 4$, and M2 is RND.IFD generated by the Inspection System.

The result of the signature computation MUST be a signature σ without the non-recoverable message part M2.

eMRTDs SHOULD implement the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.6 and SHOULD NOT make use of the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.4. eMRTDs SHALL NOT implement other signature generation schemes.

Inspection systems SHALL implement the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.6 and SHOULD implement the signature generation scheme specified in [ISO/IEC 9796-2] paragraph B.4.

6.1.2.3 ECDSA

For ECDSA, the plain signature format according to [TR-03111] SHALL be used. Only prime curves with uncompressed points SHALL be used. A hash algorithm, whose output length is of the same length or shorter than the length of the ECDSA key in use, SHALL be used. Only SHA-224, SHA-256, SHA-384 or SHA-512 are supported as hash functions. RIPEMD-160 and SHA-1 SHALL NOT be used.

The message M to be signed is the nonce RND.IFD provided by the Inspection System.

6.1.3 Application Protocol Data Units

Active Authentication is performed by a single invocation of the INTERNAL AUTHENTICATE command as specified in [ISO/IEC 7816-4].

Command		
CLA		Context specific
INS	0x88	INTERNAL AUTHENTICATE
P1/P2	0x0000	—

Data		*RND.IFD*	REQUIRED
Response			
Data		Signature σ generated by the IC	REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol has been performed successfully.	
	Other	*Operating system dependent error* The protocol failed.	

6.1.4 Active Authentication Keys

The Active Authentication Key Pairs (KPr_{AA} and KPu_{AA}) SHALL be generated in a secure way.

Both the Active Authentication Public Key (KPu_{AA}) and the Active Authentication Private Key (KPr_{AA}) are stored in the eMRTD's contactless IC. After that, no Key Management is applicable for these keys.

Note.— It should be noted that when using key lengths exceeding 1 848 bits (if Secure Messaging with 3DES is used) / 1 792 bits (if Secure Messaging with AES is used) in Active Authentication with Secure Messaging, Extended Length APDUs MUST be supported by the eMRTD chip and the Inspection System.

Issuing States or organizations SHALL choose appropriate key lengths offering protection against attacks for the life time of the eMRTD. Suitable cryptographic catalogues SHOULD be taken into account.

6.1.5 Active Authentication Public Key Info

The Active Authentication Public Key is stored in the LDS Data Group 15. The format of the structure (`SubjectPublicKeyInfo`) is specified in [RFC 5280], see Section 9.1. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

```
ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo
```

6.1.6 Inspection Process

When an eMRTD with Data Group 15 is offered to the inspection system, the Active Authentication mechanism MAY be performed to ensure that the data are read from the genuine contactless IC and that the contactless IC and physical document belong to each other.

The inspection system and the contactless IC perform the following steps:

1. The entire MRZ is read visually from the eMRTD (if not already read as part of the Basic Access Control procedure) and compared with the MRZ value in Data Group 1. Since the authenticity and integrity of Data Group 1 have been checked through Passive Authentication, similarity ensures that the visual MRZ is authentic and unchanged.

2. Passive Authentication has also proven the authenticity and integrity of Data Group 15. This ensures that the Active Authentication Public Key (KPu_{AA}) is authentic and unchanged.

3. To ensure that the Document Security Object (SO_D) is not a copy, the inspection system uses the eMRTD's Active Authentication Key pair (KPr_{AA} and KPu_{AA}) in a challenge-response protocol with the eMRTD's contactless IC as described above.

After a successful challenge-response protocol, it is proven that the Document Security Object (SO_D) belongs to the physical document, the contactless IC is genuine and contactless IC and physical document belong to each other.

6.2 Chip Authentication

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the eMRTD chip.

The main differences to Active Authentication are:

- Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
- Besides authentication of the eMRTD chip this protocol also provides strong session keys.

Details on Challenge Semantics are described in Appendix C.

The static Chip Authentication Key Pair(s) MUST be stored on the eMRTD chip.

- The private key SHALL be stored securely in the eMRTD chip's memory.
- The public key SHALL be provided as `SubjectPublicKeyInfo` in the `ChipAuthenticationPublicKeyInfo` structure (see Section 9.2.6).

The protocol provides implicit authentication of both the eMRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

If the IC supports Chip Authentication, the IC MAY support Chip Authentication in the Master File and/or MAY support Chip Authentication in the eMRTD Application. If Chip Authentication is used in conjunction with accessing data groups in LDS2 Applications, the IC MUST support Chip Authentication in the Master File.

Note.— If compatibility with European Union Extended Access Control [TR-03110] is required, the IC MUST support Chip Authentication in the eMRTD Application.

6.2.1 Protocol Specification

The following steps are performed by the terminal and the eMRTD chip.

1. The eMRTD chip sends its static Diffie-Hellman public key PK_{IC}, and the domain parameters D_{IC} to the terminal.
2. The terminal generates an ephemeral Diffie-Hellman key pair $(SK_{DH,IFD}, PK_{DH,IFD}, D_{IC})$ and sends the ephemeral public key $PK_{DH,IFD}$ to the eMRTD chip.
3. Both the eMRTD chip and the terminal compute the following:

a) The shared secret K = **KA**$(SK_{IC}, PK_{DH,IFD}, D_{IC})$ = **KA**$(SK_{DH,IFD}, PK_{IC}, D_{IC})$

b) The session keys KS_{MAC} = **KDF**$_{MAC}(K)$ and KS_{Enc} = **KDF**$_{Enc}(K)$ derived from K for Secure Messaging.

A simplified version is shown in Figure 3:

IC (chip)		***IFD (Inspection system)***
Static key pair $(SK_{IC}, PK_{IC}, D_{IC})$		
	— PK_{IC}, D_{IC} →	
		Choose random ephemeral key pair $(SK_{DH,IFD}, PK_{DH,IFD}, D_{IC})$
	← $PK_{DH,IFD}$ —	
K = **KA**$(SK_{IC}, PK_{DH,IFD}, D_{IC})$		K = **KA**$(SK_{DH,IFD}, PK_{IC}, D_{IC})$

Figure 3. Chip Authentication

To verify the authenticity of the PK_{IC} the terminal SHALL perform Passive Authentication.

6.2.2 Security Status

If Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys KS_{MAC} and KS_{Enc}. Otherwise, Secure Messaging is continued using the previously established session keys (PACE or Basic Access Control).

Note.— Passive Authentication MUST be performed in combination with Chip Authentication. Only after a successful validation of the respective Security Object may the eMRTD chip be considered genuine.

6.2.3 Cryptographic Specifications

Particular algorithms are selected by the issuing State or organization. The inspection system MUST support all combinations described in the following subsections. The eMRTD chip MAY support more than one combination of algorithms.

6.2.3.1 Chip Authentication with DH

For Chip Authentication with DH the respective algorithms and formats from Section 9.6 and Table 5 MUST be used. For Public Keys, PKCS#3 [PKCS#3] MUST be used instead of X9.42 [X9.42].

Table 5. Object Identifiers for Chip Authentication with DH

OID	***Sym. Cipher***	***Key Length***	***Secure Messaging***
id-CA-DH-3DES-CBC-CBC	3DES	112	CBC / CBC
id-CA-DH-AES-CBC-CMAC-128	AES	128	CBC / CMAC
id-CA-DH-AES-CBC-CMAC-192	AES	192	CBC / CMAC
id-CA-DH-AES-CBC-CMAC-256	AES	256	CBC / CMAC

6.2.3.2 Chip Authentication with ECDH

For Chip Authentication with ECDH the respective algorithms and formats from Section 9.6 and Table 6 MUST be used.

Table 6. Object Identifiers for Chip Authentication with ECDH

OID	***Sym. Cipher***	***Key Length***	***Secure Messaging***
id-CA-ECDH-3DES-CBC-CBC	3DES	112	CBC / CBC
id-CA-ECDH-AES-CBC-CMAC-128	AES	128	CBC / CMAC
id-CA-ECDH-AES-CBC-CMAC-192	AES	192	CBC / CMAC
id-CA-ECDH-AES-CBC-CMAC-256	AES	256	CBC / CMAC

6.2.4 Applications Protocol Data Units

Depending on the symmetric algorithm to be used, two implementations of Chip Authentication are available.

- The following command SHALL be used to implement Chip Authentication with 3DES Secure Messaging:

  1. MSE:Set KAT

- The following sequence of commands SHALL be used to implement Chip Authentication with AES Secure Messaging and MAY be used to implement Chip Authentication with 3DES Secure Messaging:

  1. MSE:Set AT
  2. GENERAL AUTHENTICATE

6.2.4.1 Implementation using MSE:Set KAT

Note.— MSE:Set KAT may only be used for `id-CA-DH-3DES-CBC-CBC` *and* `id-CA-ECDH-3DES-CBC-CBC`*, i.e. Secure Messaging is restricted to 3DES.*

Command			
CLA		Context specific	
INS	0x22	Manage Security Environment	
P1/P2	0x41A6	Set Key Agreement Template for computation.	
Data	0x91	*Ephemeral Public Key* Ephemeral public key $PK_{DH,IFD}$ (cf. Section 9.4.4) encoded as plain public key value.	REQUIRED
	0x84	*Reference of a private key* This data object is REQUIRED if the private key is ambiguous, i.e. more than one key pair is available for Chip Authentication (cf. Section 6.2 and 9.2.6).	CONDITIONAL
Response			
Data	–	Absent	
Status Bytes	0x9000	*Normal processing* The key agreement operation was successfully performed. New session keys have been derived.	
	0x6A80	*Incorrect Parameters in the command data field* The validation of the ephemeral public key failed.	
	other	*Operating system dependent error* The previously established session keys remain valid.	

6.2.4.2 Implementation using MSE:Set AT and GENERAL AUTHENTICATE

1. MSE:Set AT: The command MSE:Set AT is used to select and initialize the protocol. The use of MSE:Set AT for Chip Authentication is indicated by a Chip Authentication Object Identifier (see section 6.2.3 and 9.2.7) contained as cryptographic mechanism reference with tag 0x80, see below.

Command			
CLA		Context specific	
INS	0x22	Manage Security Environment	
P1/P2	0x41A4	*Chip Authentication*: Set Authentication Template for internal authentication.	
Data	0x80	*Cryptographic mechanism reference* Object Identifier of the protocol to select (value only, Tag 0x06 is omitted).	REQUIRED

	0x84	*Reference of a private key* This data object is REQUIRED to indicate the identifier of the private key to be used if the private key is ambiguous, i.e. more than one private key is available for Chip Authentication.	CONDITIONAL
Response			
Data	–	Absent	
Status Bytes	0x9000	*Normal processing* The protocol has been selected and initialized.	
	0x6A80	*Incorrect parameters in the command data field* Algorithm not supported or initialization failed.	
	0x6A88	*Referenced data not found* The referenced data (i.e. private key) is not available.	
	other	*Operating system dependent error* The initialization of the protocol failed.	

Note.— Some operating systems accept the selection of an unavailable key and return an error only when the key is used for the selected purpose.

2. GENERAL AUTHENTICATE: The command GENERAL AUTHENTICATE is used to perform the Chip Authentication.

Command				
CLA		Context specific		
INS	0x86	GENERAL AUTHENTICATE		
P1/P2	0x0000	Keys and protocol implicitly known.		
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects.		REQUIRED
		0x80	Ephemeral Public Key	
Response				
Data	0x7C	*Dynamic Authentication Data* Protocol specific data objects		REQUIRED
Status Bytes	0x9000	*Normal processing* The protocol (step) was successful.		
	0x6300	*Authentication failed* The protocol (step) failed.		

	0x6A80	*Incorrect parameters in data field* Provided data is invalid.
	0x6A88	*Referenced data not found* The referenced data (i.e. private key) is not available.
	other	*Operating system dependent error* The protocol (step) failed.

Note.— The public keys for Chip Authentication supported by the chip are made available in the Security Object (see Section 9.2.11). If more than one public key is supported, the terminal MUST select the corresponding private key of the chip to be used within MSE:Set AT.

6.2.4.3 Ephemeral Public Key

The ephemeral public keys (cf. Section 9.4.4) SHALL be encoded as elliptic curve point (ECDH) or unsigned integer (DH).

7. ADDITIONAL ACCESS CONTROL MECHANISMS

The personal data stored in the contactless IC as defined to be the mandatory minimum for global interoperability are the MRZ and the digitally stored image of the bearer's face. Both items can also be seen (read) visually after the eMRTD has been opened and offered for inspection.

Besides the digitally stored image of the face as the primary biometric for global interoperability, ICAO has endorsed the use of digitally stored images of fingers and/or irises in addition to the face. For national or bilateral use, States MAY choose to store templates and/or MAY choose to limit access or encrypt this data, as to be decided by States themselves.

Access to this more sensitive personal data SHOULD be more restricted. This can be accomplished in two ways: extended access control or data encryption. Section 7.1. specifies Terminal Authentication as an interoperable mechanism for extended access control. If no interoperability is required, other mechanisms can be used.

7.1 Terminal Authentication

The Terminal Authentication mechanism is CONDITONAL. Implementation is REQUIRED for LDS2 applications. Terminal Authentication MAY be used to protect secondary biometrics in the eMRTD Application.
The Terminal Authentication Protocol is a two move challenge-response protocol that provides explicit unilateral authentication of the terminal. The protocol is based on Extended Access Control as specified in [TR-03110]. If this protocol is supported by the IC, it MUST support Chip Authentication or PACE with Chip Authentication Mapping.

This protocol enables the IC to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication or PACE with Chip Authentication Mapping. The IC MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

The IC MAY support Terminal Authentication in the Master File and/or the eMRTD Application. If Terminal Authentication is used to protect data groups in other applications than the eMRTD Application, the IC MUST support Terminal Authentication in the Master File.

Note.— If compatibility with European Union Extended Access Control [TR-03110] is required, the IC MUST support Terminal Authentication in the eMRTD Application.

7.1.2 Protocol Specification

The following steps are performed by the terminal and the IC:

1. The terminal sends a certificate chain to the IC. The chain starts with a certificate verifiable with the CVCA public key stored on the chip and ends with the Terminal Certificate.

2. The IC verifies the certificates and extracts the terminal's public key PK_{IFD}.

3. The IC randomly chooses a challenge r_{IC} and sends it to the terminal.

4. The terminal responds with the signature s_{IFD} = **Sign***(SK_{IFD}, $ID_{IC}||r_{IC}||$***Comp***($PK_{DH,IFD}$))*.

5. The IC checks that **Verify***(PK_{IFD} , s_{IFD}, $ID_{IC}||r_{IC}||$***Comp***($PK_{DH,IFD}$)) = true*.

Note.— The key $PK_{DH,IFD}$ is generated during Chip Authentication or PACE with Chip Authentication Mapping. If more than one key is generated (e.g. Chip Authentication is performed after PACE with Chip Authentication Mapping), the newest key MUST be used.

In this protocol ID_{IC} is an identifier of the IC:

- If BAC is used ID_{IC} is the eMRTD's Document Number as contained in the MRZ including the check digit.

- If PACE is used, ID_{IC} is computed using the IC's ephemeral PACE public key, i.e. ID_{IC} = **Comp***($PK_{DH,IC}$)*.

Note.— A successful execution of the PACE protocol is REQUIRED before Terminal Authentication can be performed in the MF.

A simplified version is shown below:

IC (chip)		**IFD (inspection system)**
Choose r_{IC} randomly		
	–- r_{IC} →	
		s_{IFD} = **Sign***(SK_{IFD},$ID_{IC}||r_{IC}||$***Comp***($PK_{DH,IFD}$))*
	← s_{IFD} –-	
Verify*(PK_{IFD} , s_{IFD}, $ID_{IC}||r_{IC}||$***Comp***($PK_{DH,IFD}$)) = true*		

Figure 4: Terminal Authentication

7.1.3 Security Status

If Terminal Authentication was successfully performed, the IC SHALL grant access to stored sensitive data according to the effective authorization of the authenticated terminal. If the effective authorization does not grant access rights to any data in a LDS2 Application, selecting this application MUST be rejected by the IC.

The IC SHALL however restrict the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key, i.e. the ephemeral public key provided by the terminal as part of Chip Authentication or PACE with

Chip Authentication Mapping. The IC MUST NOT accept more than one execution of Terminal Authentication within the same session (cf. Section 9.8.1 and Section 9.8.3 on the definition of “session”).

Note.— Access rights are valid as long as the Secure Messaging established by the authenticated ephemeral public keys is active, therefore the security status is not affected by selecting or deselecting applications.

Note.— Secure Messaging is not affected by Terminal Authentication. The eMRTD chip SHALL retain Secure Messaging even if Terminal Authentication fails (unless a Secure Messaging error occurs).

7.1.4 Cryptographic Specifications

7.1.4.1 Terminal Authentication with RSA

For Terminal Authentication with RSA the following algorithms and formats MUST be used.

7.1.4.1.1 Signature Algorithm

RSA [RFC-3447], [PKCS#1] as specified in Table 7 SHALL be used.

Table 7. Object Identifiers for Terminal Authentication with RSA

OID	Signature	Hash	Parameters
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	default
id-TA-RSA-PSS-SHA-512	RSASSA-PSS	SHA-512	default

The default parameters to be used with RSA-PSS are defined as follows:

- Hash Algorithm: The hash algorithm is selected according to Table 7.
- Mask Generation Algorithm: MGF1 [RFC-3447], [PKCS#1] using the selected hash algorithm.
- Salt Length: Octet length of the output of the selected hash algorithm.
- Trailer Field: 0xBC

7.1.4.1.2 Public Key Format

The TLV-Format [ISO/IEC 7816-8] as described in Doc 9303-12 SHALL be used.

- The object identifier SHALL be taken from Table 7.
- The bit length of the modulus SHALL be 2048, or 3072.
- The bit length of the exponent SHALL be at most 32.

7.1.4.1.3 Public Key Compression

The terminal's compressed ephemeral public key **Comp**$(PK_{DH,IFD})$ is defined as the SHA-1 hash of the DH public value, i.e. an octet string of fixed length 20.

7.1.4.2 Terminal Authentication with ECDSA

For Terminal Authentication with ECDSA the following algorithms and formats MUST be used.

7.1.4.2.1 Signature Algorithm

ECDSA with plain signature format [TR-03111] as specified in Table 8 SHALL be used.

Table 8. Object Identifiers for Terminal Authentication with ECDSA

OID	Signature	Hash
id-TA-ECDSA-SHA-224	ECDSA	SHA-224
id-TA-ECDSA-SHA-256	ECDSA	SHA-256
id-TA-ECDSA-SHA-384	ECDSA	SHA-384
id-TA-ECDSA-SHA-512	ECDSA	SHA-512

7.1.4.2.2 Public Key Format

The TLV-Format [ISO/IEC 7816-8] as described in Doc 9303-12 SHALL be used.

- The object identifier SHALL be taken from Table 8.
- The bit length of the curve SHALL be 224, 256, 320, 384 or 512.
- Domain Parameters SHALL be compliant to [TR-03111].

7.1.4.2.3 Public Key Compression

The terminal's compressed ephemeral public key **Comp**$(PK_{DH,IFD})$ is defined as the x-coordinate of the ECDH public point, i.e. an octet string of fixed length ⌈log256p⌉.

7.1.4.3 Certificate Validation

To validate a Terminal Certificate, the IC MUST be provided with a certificate chain starting at a trust-point stored on the IC. Those trust-points are more or less recent public keys of the IC's CVCA.

7.1.4.3.1 Initial State of the IC's trust-point(s)

The initial trust-point(s) SHALL be stored securely in the IC's memory in the production or (pre-) personalization phase.

The (pre-)personalization agent SHALL

- set the current date of the IC to the date of the (pre-)personalization, and
- personalize the CVCA key with the most recent effective date as trust-point.

The (pre-)personalization agent MAY additionally personalize the previous CVCA key as trust-point.

7.1.4.3.2 Link Certificates

As the key pair used by the CVCA changes over time, CVCA Link Certificates have to be produced. CVCA Link Certificates MUST be signed with the previous CVCA key, i.e. the CVCA key with the most recent effective date. The IC is REQUIRED to internally update its trust-point(s) according to received valid link certificates.

The IC MUST be able to store up to two trust-points.

Note.— Due to the scheduling of CVCA Link Certificates (see Doc 9303-12), at most two trust-points need to be stored on the IC.

7.1.4.3.3 Current Date

The IC MUST accept expired CVCA Link Certificates but it MUST NOT accept expired DV and Terminal Certificates. To determine whether a certificate is expired, the IC SHALL use its *current date*.

Current Date: If the IC has no internal clock, the current date of the IC SHALL be approximated as described in the following. The date is autonomously approximated by the IC using the most recent certificate effective date contained in a valid CVCA Link Certificate, a DV Certificate or an *Accurate Terminal Certificate*.

Accurate Terminal Certificate: A Terminal Certificate is accurate if the issuing Document Verifier (DV) is trusted by the IC to produce Terminal Certificates with the correct certificate effective date. CVCA Link Certificates, DV Certificates and Terminal Certificates issued by a domestic DV SHALL be considered accurate by the IC. Other certificates MUST NOT be considered accurate.

A terminal MAY send CVCA Link Certificates, DV Certificates, and Terminal Certificates to an IC to update the current date and the trust-point stored on the IC even if the terminal does not intend to or is not able to continue with Terminal Authentication.

Note.— The IC only verifies that a certificate is apparently recent (i.e. with respect to the approximated current date), unless the IC contains an internal clock.

7.1.4.3.4 General Validation Procedure

The certificate validation procedure consists of three steps:

1. **Certificate Verification:** The signature MUST be valid and unless the certificate is a CVCA Link Certificate, the certificate MUST NOT be expired. If the verification fails, the procedure SHALL be aborted.

   Note: The case of an expired CVCA Link Certificate can only occur if the IC has a source of time beyond the approximated current date described above.

2. **Internal Status Update:** The current date MUST be *updated*, the public key and the attributes (including relevant certificate extensions) MUST be imported, new trust-points MUST be *enabled*, expired trust-points MUST be *disabled* for the verification of DV Certificates.

3. **Cleanup:** The chip SHALL provide at most two enabled trust-points per application. If more than two trust-points for an application remain enabled after the internal status update, the trust-point with the least recent effective date SHALL be *disabled*.

The operation of *updating* the current date and the operations of *enabling* and *disabling* a trust-point MUST be implemented as an atomic operation.

Enabling a trust-point: The new trust-point SHALL be added to the list of trust-points.

Disabling a trust-point: Expired trust-points MUST NOT be used for the verification of DV Certificates. In case of ICs where the current date may be advanced beyond the expiry date of a trust-point, e.g. ICs using an internal clock, expired trust-points MUST remain usable for the verification of CVCA Link Certificates. Disabled trust-points MAY be deleted after the successful import of the successive Link Certificate.

7.1.4.3.5 Example Validation Procedure

The following validation procedure, provided as an example, MAY be used to validate a certificate chain. For each received certificate the IC performs the following steps:

1. The IC verifies the signature on the certificate. If the signature is incorrect, the verification fails.

2. If the certificate is not a CVCA Link Certificate, the certificate expiration date is compared to the IC's current date. If the expiration date is before the current date, the verification fails.

3. The certificate is accepted as valid and the public key and the attributes (including relevant certificate extensions) contained in the certificate are imported.

    - For CVCA, DV, and Accurate Terminal Certificates: The certificate effective date is compared to the IC's current date. If the current date is before the effective date, the current date is updated to the effective date.

    - For CVCA Link Certificates: The new CVCA public key is added to the list of trust-points stored securely in the IC's memory. The new trust-point is then enabled.

    - For DV and Terminal Certificates: The new DV or terminal public key is temporarily imported for subsequent certificate verification or Terminal Authentication, respectively.

4. Expired trust-points stored securely in the IC's memory are disabled for the verification of DV Certificates and may be removed from the list of trust-points.

7.1.4.3.6 Effective Authorization

Each certificate SHALL contain a *Certificate Holder Authorization Template* (see Doc9303-12) and MAY contain *Authorization Extensions* (see Doc9303-12, section 7.2.2.6).

- The Certificate Holder Authorization Template identifies the terminal type (this specification only considers Inspection Systems, but other specifications may use different terminal types).

- The Certificate Holder Authorization Template and the Authorization Extensions determine the *relative authorization* of the certificate holder assigned by the issuing certificate authority.

To determine the *effective authorization* of a certificate holder, the IC MUST calculate a bitwise Boolean 'and' of the relative authorization contained in the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate.

The effective authorization SHALL be interpreted by the IC as follows:

- The effective role is a CVCA:

    - This link certificate was issued by the national CVCA.

- The IC MUST update its internal trust-point, i.e. the public key and the effective authorization.
- The certificate issuer is a trusted source of time and the IC MUST update its current date using the Certificate Effective Date.
- The IC MUST NOT grant the CVCA access to sensitive data (i.e. the effective authorization SHOULD be ignored).

- The effective role is a DV:
  - The certificate was issued by the national CVCA for an authorized DV.
  - The certificate issuer is a trusted source of time and the IC MUST update its current date using the Certificate Effective Date.
  - The IC MUST NOT grant a DV access to sensitive data (i.e. the effective authorization SHOULD be ignored).

- The effective role is a Terminal:
  - The certificate was issued by either a domestic or a foreign DV.
  - If the certificate is an accurate terminal certificate (cf. Section 7.1.4.3.3), the issuer is a trusted source of time and the IC MUST update its current date using the Certificate Effective Date.
  - The IC MUST grant the authenticated terminal access to sensitive data according to the effective authorization.

Note.— The Certificate Holder Authorization Template and the Authorization Extensions can contain bits not allocated to an access right (RFU bits). The IC MUST ignore these bits during evaluation of access rights.

7.1.4.3.7 Public Key Import

Public keys imported by the certificate validation procedure are either *permanently* or *temporarily* stored on the IC.

The IC SHOULD reject to import a public key, if the Certificate Holder Reference is already known to the IC.

Permanent Import: Public keys contained in CVCA Link Certificates SHALL be permanently imported by the IC and MUST be stored securely in the IC's memory. A permanently imported public key and its metadata SHALL fulfill the following conditions:

- It MAY be overwritten *after expiration* by a subsequent permanently imported public key.
- It either MUST be overwritten by a subsequent permanently imported public key with the same Certificate Holder Reference or the import MUST be rejected.
- It MUST NOT be overwritten by a temporarily imported public key.

Enabling and disabling a permanently imported public key MUST be an atomic operation.

Temporary Import: Public keys contained in DV and Terminal Certificates SHALL be temporarily imported by the IC. A temporarily imported public key and its metadata SHALL fulfill the following conditions:

- It SHALL NOT be selectable or usable after a power down of the IC.
- It MUST remain usable until the subsequent cryptographic operation is successfully completed (i.e. PSO:Verify Certificate or External Authenticate).
- It MAY be overwritten by a subsequent temporarily imported public key.

A terminal MUST NOT make use of any temporarily imported public key but the most recently imported.

Imported Metadata: For each permanently or temporarily imported public key the following additional data contained in the certificate (see Doc 9303-12) MUST be stored:

- Certificate Holder Reference
- Certificate Holder Authorization (effective role and effective authorization)
- Certificate Effective Date
- Certificate Expiration Date
- Certificate Extensions (where applicable)

The calculation of the effective role (CVCA, DV, or Terminal) and the effective authorization of the certificate holder is described in Section 7.1.4.3.6.

Note.— The format of the stored data is operating system dependent and out of the scope of this specification.

7.1.5 Application Protocol Data Units

The following sequence of commands SHALL be used with secure messaging to implement Terminal Authentication:

- MSE:Set DST
- PSO:Verify Certificate
- MSE:Set AT
- Get Challenge
- External Authenticate

Steps 1 and 2 are repeated for every CV certificate to be verified (CVCA Link Certificates, DV Certificate, Terminal Certificate).

7.1.5.1 MSE:Set DST

The command MSE:Set DST is used to setup certificate verification.

Command

CLA		Context Specific	
INS	0x22	Manage Security Environment	
P1/P2	0x81B6	Set Digital Signature Template for verification.	
Data	0x83	*Reference of a public key* ISO 8859-1 encoded name of the public key to be set	REQUIRED

Response		
Data	–	Absent
Status Bytes	0x9000	*Normal Operation* The key has been selected for the given purpose.
	0x6A88	*Referenced data not found* The selection failed as the public key is not available.
	other	*Operating system dependent error* The key has not been selected.

Note.— Some operating systems accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.

7.1.5.2 PSO:Verify Certificate

The command PSO:Verify Certificate is used to verify and import certificates.

Command			
CLA		Context Specific	
INS	0x2A	Perform Security Operation	
P1/P2	0x00BE	Verify self-descriptive certificate.	
Data	0x7F4E	*Certificate body* The body of the certificate to be verified.	REQUIRED
	0x5F37	*Signature* The signature of the certificate to be verified.	REQUIRED

Response		
Data	–	Absent
Status Bytes	0x9000	*Normal processing* The certificate was successfully validated and the public key has been imported.
	other	*Operating system dependent error* The public key could not be imported (e.g. the certificate was not accepted).

7.1.5.3 MSE:Set AT

The use of MSE:Set AT for Terminal Authentication is indicated by P1/P2 set to 0x81A4, see below.

Command		
CLA		Context Specific
INS	0x22	Manage Security Environment
P1/P2	0x81A4	*Terminal Authentication:*

		Set Authentication Template for external authentication.	
Data	0x83	*Reference of a public key / secret key* This data object is used to select the public key of the terminal by its ISO 8859-1 encoded name.	REQUIRED

Response		
Data	–	Absent
Status Bytes	0x9000	*Normal processing* The protocol has been selected and initialized.
	0x6A80	*Incorrect parameters in the command data field* Algorithm not supported or initialization failed.
	0x6A88	*Referenced data not found* The referenced data is not available.
	other	*Operating system dependent error* The initialization of the protocol failed.

Note.— Some operating systems accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.

7.1.5.4 Get Challenge

Command			
CLA		Context Specific	
INS	0x84	Get Challenge	
P1/P2	0x0000		
Data	–	Absent	
Le	0x08		REQUIRED

Response		
Data	r_{IC}	8 bytes of randomness.
Status Bytes	0x9000	*Normal processing*
	other	*Operating system dependent error*

7.1.5.5 External Authenticate

Command			
CLA		Context Specific	
INS	0x82	External Authenticate	
P1/P2	0x0000	Keys and Algorithms implicitly known.	
Data		Signature generated by the terminal.	REQUIRED

Response		
Data	–	Absent

Response		
Status Bytes	0x9000	*Normal processing* The authentication was successful. Access to data groups will be granted according to the effective authorization of the corresponding verified certificate.
	0x6300	*Warning* Signature verification failed.
	0x6982	*Security status not satisfied* The authentication failed as the current authentication level of the terminal does not allow to use Terminal Authentication (e.g. Terminal Authentication was already performed, etc.).
	other	*Operating system dependent error* The authentication failed.

7.2 Encryption of Additional Biometrics

Restricting access to the additional biometrics MAY also be done by encrypting them. To be able to decrypt the encrypted data, the inspection system MUST be provided with a decryption key. Defining the encryption/decryption algorithm and the keys to be used is up to the implementing State and is outside the scope of this document.

The implementation of the protection of the additional biometrics depends on the State's internal specifications or the bilaterally agreed specifications between States sharing this information.

8. INSPECTION SYSTEM

In order to support the required functionality and the defined options that can be implemented on eMRTDs that will be offered, the inspection system will have to meet certain pre-conditions.

8.1 Basic Access Control

Inspection systems supporting Basic Access Control MUST meet the following pre-conditions:

1. The inspection system is equipped with means to acquire the MRZ from the physical document to derive the Document Basic Access Keys (K_{Enc} and K_{MAC}) from the eMRTD.

2. The inspection system's software supports the protocol described in Section 4.3, in the case that an eMRTD with Basic Access Control is offered to the system, including the encryption of the communication channel with Secure Messaging.

8.2 Password Authenticated Connection Establishment

Inspection systems supporting PACE MUST meet the following pre-conditions:

1. The inspection system is equipped with means to acquire the MRZ and/or the CAN from the physical document.

2. The inspection system's software supports the protocol described in Section 4.4, in the case that an eMRTD with PACE is offered to the system, including the encryption of the communication channel with Secure

Messaging.

8.3 Passive Authentication

To be able to perform a passive authentication of the data stored in the eMRTDs contactless IC, the inspection system needs to have knowledge of key information of the issuing States or organizations:

1. For each issuing State or organization, the Country Signing CA Certificate or the relevant information extracted from the certificate SHALL be securely stored in the inspection system.

2. Alternatively, for each issuing State or organization, the Document Signer Certificates (C_{DS}) or the relevant information extracted from the certificates SHALL be securely stored in the inspection system.

Before using a Country Signing CA Public Key of an issuing State or organization, trust in this key MUST be established by the receiving State or organization.

Before using a Document Signer Certificate (C_{DS}) for verification of a SO_D, the inspection system SHALL verify its digital signature, using the Country Signing CA Public Key.

Additionally, inspection systems SHALL have access to verified revocation information.

8.4 Active Authentication

Support of Active Authentication by inspection systems is OPTIONAL.

If the inspection system supports Active Authentication, it is REQUIRED that the inspection system have the ability to read the visual MRZ.

If the inspection system supports Active Authentication, the inspection system's software SHALL support the Active Authentication protocol described in Section 6.1.

8.5 Chip Authentication

Support of Chip Authentication by inspection systems is OPTIONAL.

If the inspection system supports Chip Authentication, it is REQUIRED that the inspection system have the ability to read the visual MRZ.

If the inspection system supports Chip Authentication, the inspection system's software SHALL support the Chip Authentication protocol described in Section 6.2.

8.6 Terminal Authentication

Support of Terminal Authentication by inspection systems is OPTIONAL.

If the inspection system supports Terminal Authentication, it is REQUIRED that the inspection system has the capability to securely store the private key of the inspection system. The inspection system MUST have access to its DV in regular

intervals to renew the terminal certificate.

If the inspection system supports Terminal Authentication, the inspection system's software SHALL support the Terminal Authentication protocol as described in section 7.1.

8.7 Decryption of Additional Biometrics

The implementation of the protection of the optional additional biometrics depends on the State’s internal specifications or the bilaterally agreed specifications between States sharing this information.

9. COMMON SPECIFICATIONS

9.1 ASN.1 Structures

The data structures `SubjectPublicKeyInfo` and `AlgorithmIdentifier` are defined as follows:

```
SubjectPublicKeyInfo ::= SEQUENCE {
  algorithm  AlgorithmIdentifier,
  subjectPublicKey    BIT STRING
}

AlgorithmIdentifier ::= SEQUENCE {
  algorithm OBJECT IDENTIFIER,
  parameters ANY DEFINED BY algorithm OPTIONAL
}
```

Details on the `parameters` can be found in [X9.42] and [TR-03111].

9.2 Information on Supported Protocols and Supported Applications

The ASN.1 data structure `SecurityInfos` SHALL be provided by the eMRTD chip to indicate supported security protocols. The data structure is specified as follows:

```
SecurityInfos  ::= SET OF SecurityInfo

SecurityInfo ::= SEQUENCE {
  protocol  OBJECT IDENTIFIER,
  requiredData ANY DEFINED BY protocol,
  optionalData ANY DEFINED BY protocol OPTIONAL
}
```

The elements contained in a `SecurityInfo` data structure have the following meaning:

- The object identifier `protocol` identifies the supported protocol.
- The open type `requiredData` contains protocol specific mandatory data.
- The open type `optionalData` contains protocol specific optional data.

Security Infos for PACE

To indicate support for PACE `SecurityInfos` may contain the following entries:

- At least one `PACEInfo` using a standardized domain parameter MUST be present.
- For each supported set of explicit domain parameters a `PACEDomainParameterInfo` MUST be present.

Security Infos for Active Authentication

If ECDSA based signature algorithm is used for Active Authentication by the eMRTD chip, the `SecurityInfos` MUST contain the following `SecurityInfo` entry:

- `ActiveAuthenticationInfo`

Security Infos for Chip Authentication

To indicate support for Chip Authentication `SecurityInfos` may contain the following entries:

- At least one `ChipAuthenticationInfo` and the corresponding `ChipAuthenticationPublicKeyInfo` using explicit domain parameters MUST be present.

Security Infos for Terminal Authentication

To indicate support for Terminal Authentication `SecurityInfos` may contain the following entry:

- At least one `TerminalAuthenticationInfo` SHALL be present.

Security Infos for present Applications

Doc 9303-10 section 3.11.2 recommends the presence of a transparent elementary file EF.DIR to indicate supported applications. The file is mandatory if any LDS2 Application is present. Since EF.DIR is not signed and can therefore be manipulated, e.g. to hide existing applications from the IFD, a secured copy of EF.DIR is provided as `SecurityInfo` if any LDS2 Application is present.

Security Infos for Other Protocols

`SecurityInfos` MAY contain additional entries indicating support for other protocols or providing other information. The inspection system MAY discard any unknown entry.

9.2.1 PACEInfo

This data structure provides detailed information on an implementation of PACE.

- The object identifier `protocol` SHALL identify the algorithms to be used (i.e. key agreement, symmetric cipher and MAC).
- The integer `version` SHALL identify the version of the protocol. Only version 2 is supported by this specification.
- The integer `parameterId` is used to indicate the domain parameter identifier. It MUST be used if the eMRTD chip uses standardized domain parameters (cf. Section 9.5.1), provides multiple explicit domain parameters for PACE or `protocol` is one of the `*-CAM-*` OIDs. In case of PACE with Chip Authentication Mapping, the `parameterID` also denotes the ID of the Chip Authentication key used, i.e. the chip MUST provide a `ChipAuthenticationPublicKeyInfo` with `keyID` equal to `parameterID` from this data structure.

```
PACEInfo ::= SEQUENCE {
    protocol    OBJECT IDENTIFIER(
```

```
                id-PACE-DH-GM-3DES-CBC-CBC |
                id-PACE-DH-GM-AES-CBC-CMAC-128 |
                id-PACE-DH-GM-AES-CBC-CMAC-192 |
                id-PACE-DH-GM-AES-CBC-CMAC-256 |
                id-PACE-ECDH-GM-3DES-CBC-CBC |
                id-PACE-ECDH-GM-AES-CBC-CMAC-128 |
                id-PACE-ECDH-GM-AES-CBC-CMAC-192 |
                id-PACE-ECDH-GM-AES-CBC-CMAC-256 |
                id-PACE-DH-IM-3DES-CBC-CBC |
                id-PACE-DH-IM-AES-CBC-CMAC-128 |
                id-PACE-DH-IM-AES-CBC-CMAC-192 |
                id-PACE-DH-IM-AES-CBC-CMAC-256 |
                id-PACE-ECDH-IM-3DES-CBC-CBC |
                id-PACE-ECDH-IM-AES-CBC-CMAC-128 |
                id-PACE-ECDH-IM-AES-CBC-CMAC-192 |
                id-PACE-ECDH-IM-AES-CBC-CMAC-256 |
                id-PACE-ECDH-CAM-AES-CBC-CMAC-128 |
                id-PACE-ECDH-CAM-AES-CBC-CMAC-192 |
                id-PACE-ECDH-CAM-AES-CBC-CMAC-256),
    version     INTEGER, -- MUST be 2
    parameterId INTEGER OPTIONAL
}
```

9.2.2 PACEDomainParameterInfo

This data structure is REQUIRED if the eMRTD chip provides explicit domain parameters for PACE and MUST be omitted otherwise.

- The object identifier `protocol` SHALL identify the type of the domain parameters (i.e. DH or ECDH).
- The sequence `domainParameter` SHALL contain the domain parameters.
- The integer `parameterId` MAY be used to indicate the local domain parameter identifier. It MUST be used if the eMRTD chip provides multiple explicit domain parameters for PACE.

```
PACEDomainParameterInfo ::= SEQUENCE {
  protocol          OBJECT IDENTIFIER(
                    id-PACE-DH-GM |
                    id-PACE-ECDH-GM |
                    id-PACE-DH-IM |
                    id-PACE-ECDH-IM |
                    id-PACE-ECDH-CAM),
  domainParameter   AlgorithmIdentifier,
  parameterId       INTEGER OPTIONAL
}
```

Note.— The eMRTD chip MAY support more than one set of explicit domain parameters (i.e. the chip may support different algorithms and/or key lengths). In this case the identifier MUST be disclosed in the corresponding `PACEDomainParameterInfo`.

Domain parameters contained in `PACEDomainParameterInfo` are unprotected and may be insecure. Using insecure

domain parameters for PACE will leak the used password. eMRTD chips MUST support at least one set of standardized domain parameters as specified in Section 9.5.1. Inspection systems MUST NOT use explicit domain parameters provided by the eMRTD chip unless those domain parameters are explicitly known to be secure by the inspection systems.

Ephemeral public keys MUST be exchanged as plain public key values. More information on the encoding can be found in Section 09.4.4.

9.2.3 PACE Object Identifier

The object identifiers used for PACE are contained in the subtree of `bsi-de`:

```
bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}
```

The following Object Identifier SHALL be used:

```
id-PACE OBJECT IDENTIFIER ::= {
    bsi-de protocols(2) smartcard(2) 4
}

id-PACE-DH-GM                     OBJECT IDENTIFIER ::= {id-PACE 1}
id-PACE-DH-GM-3DES-CBC-CBC        OBJECT IDENTIFIER ::= {id-PACE-DH-GM 1}
id-PACE-DH-GM-AES-CBC-CMAC-128    OBJECT IDENTIFIER ::= {id-PACE-DH-GM 2}
id-PACE-DH-GM-AES-CBC-CMAC-192    OBJECT IDENTIFIER ::= {id-PACE-DH-GM 3}
id-PACE-DH-GM-AES-CBC-CMAC-256    OBJECT IDENTIFIER ::= {id-PACE-DH-GM 4}

id-PACE-ECDH-GM                   OBJECT IDENTIFIER ::= {id-PACE 2}
id-PACE-ECDH-GM-3DES-CBC-CBC      OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 1}
id-PACE-ECDH-GM-AES-CBC-CMAC-128  OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 2}
id-PACE-ECDH-GM-AES-CBC-CMAC-192  OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 3}
id-PACE-ECDH-GM-AES-CBC-CMAC-256  OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 4}

id-PACE-DH-IM                     OBJECT IDENTIFIER ::= {id-PACE 3}
id-PACE-DH-IM-3DES-CBC-CBC        OBJECT IDENTIFIER ::= {id-PACE-DH-IM 1}
id-PACE-DH-IM-AES-CBC-CMAC-128    OBJECT IDENTIFIER ::= {id-PACE-DH-IM 2}
id-PACE-DH-IM-AES-CBC-CMAC-192    OBJECT IDENTIFIER ::= {id-PACE-DH-IM 3}
id-PACE-DH-IM-AES-CBC-CMAC-256    OBJECT IDENTIFIER ::= {id-PACE-DH-IM 4}

id-PACE-ECDH-IM                   OBJECT IDENTIFIER ::= {id-PACE 4}
id-PACE-ECDH-IM-3DES-CBC-CBC      OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 1}
id-PACE-ECDH-IM-AES-CBC-CMAC-128  OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 2}
id-PACE-ECDH-IM-AES-CBC-CMAC-192  OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 3}
id-PACE-ECDH-IM-AES-CBC-CMAC-256  OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 4}

id-PACE-ECDH-CAM                  OBJECT IDENTIFIER ::= {id-PACE 6}
id-PACE-ECDH-CAM-AES-CBC-CMAC-128 OBJECT IDENTIFIER ::= {id-PACE-ECDH-CAM 2}
id-PACE-ECDH-CAM-AES-CBC-CMAC-192 OBJECT IDENTIFIER ::= {id-PACE-ECDH-CAM 3}
id-PACE-ECDH-CAM-AES-CBC-CMAC-256 OBJECT IDENTIFIER ::= {id-PACE-ECDH-CAM 4}
```

9.2.4 ActiveAuthenticationInfo

If ECDSA based signature algorithm is used for Active Authentication by the eMRTD chip, the `SecurityInfos` in LDS Data Group 14 of the eMRTD chip MUST contain following `SecurityInfo` entry:

```
ActiveAuthenticationInfo ::= SEQUENCE {
  protocol           OBJECT IDENTIFIER(id-icao-mrtd-security-aaProtocolObject),
  version            INTEGER, -- MUST be 1
  signatureAlgorithm OBJECT IDENTIFIER
}

id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::=
                                    { id-icao-mrtd-security 5 }
```

For `signatureAlgorithm`, the object identifiers defined in [TR-03111] SHALL be used.

Note.— The Object Identifier `id-icao-mrtd-security` is defined in Doc 9303-10.

9.2.5 ChipAuthenticationInfo

This data structure provides detailed information on an implementation of Chip Authentication.

- The object identifier `protocol` SHALL identify the algorithms to be used (i.e. key agreement, symmetric cipher and MAC).
- The integer `version` SHALL identify the version of the protocol. Currently, only version 1 is supported by this specification.
- The integer `keyId` MAY be used to indicate the local key identifier. It MUST be used if the eMRTD chip provides multiple public keys for Chip Authentication.

```
ChipAuthenticationInfo ::= SEQUENCE {
  protocol   OBJECT IDENTIFIER(
             id-CA-DH-3DES-CBC-CBC |
             id-CA-DH-AES-CBC-CMAC-128 |
             id-CA-DH-AES-CBC-CMAC-192 |
             id-CA-DH-AES-CBC-CMAC-256 |
             id-CA-ECDH-3DES-CBC-CBC |
             id-CA-ECDH-AES-CBC-CMAC-128 |
             id-CA-ECDH-AES-CBC-CMAC-192 |
             id-CA-ECDH-AES-CBC-CMAC-256),
  version    INTEGER, -- MUST be 1
  keyId      INTEGER OPTIONAL
}
```

9.2.6 ChipAuthenticationPublicKeyInfo

This data structure provides a public key for Chip Authentication or PACE with Chip Authentication Mapping of the eMRTD chip.

- The object identifier `protocol` SHALL identify the type of the public key (i.e. DH or ECDH).
- The sequence `chipAuthenticationPublicKey` SHALL contain the public key in encoded form.
- The integer `keyId` MAY be used to indicate the local key identifier. It MUST be used if the eMRTD chip provides multiple public keys for Chip Authentication or if this key is used for PACE with Chip Authentication Mapping.

```
ChipAuthenticationPublicKeyInfo ::= SEQUENCE {
    protocol                    OBJECT IDENTIFIER(id-PK-DH | id-PK-ECDH),
    chipAuthenticationPublicKey SubjectPublicKeyInfo,
    keyId                       INTEGER OPTIONAL
}
```

Note.— The eMRTD chip MAY support more than one Chip Authentication Key Pair (i.e. the chip may support different algorithms and/or key lengths). In this case the local key identifier MUST be disclosed in the corresponding `ChipAuthenticationInfo` and `ChipAuthenticationPublicKeyInfo`.

9.2.7 Chip Authentication Object Identifier

The following Object Identifier SHALL be used:

```
id-PK OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 1
}

id-PK-DH                    OBJECT IDENTIFIER ::= {id-PK 1}
id-PK-ECDH                  OBJECT IDENTIFIER ::= {id-PK 2}

id-CA OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 3
}

id-CA-DH                    OBJECT IDENTIFIER ::= {id-CA 1}
id-CA-DH-3DES-CBC-CBC       OBJECT IDENTIFIER ::= {id-CA-DH 1}
id-CA-DH-AES-CBC-CMAC-128   OBJECT IDENTIFIER ::= {id-CA-DH 2}
id-CA-DH-AES-CBC-CMAC-192   OBJECT IDENTIFIER ::= {id-CA-DH 3}
id-CA-DH-AES-CBC-CMAC-256   OBJECT IDENTIFIER ::= {id-CA-DH 4}

id-CA-ECDH                  OBJECT IDENTIFIER ::= {id-CA 2}
id-CA-ECDH-3DES-CBC-CBC     OBJECT IDENTIFIER ::= {id-CA-ECDH 1}
id-CA-ECDH-AES-CBC-CMAC-128 OBJECT IDENTIFIER ::= {id-CA-ECDH 2}
id-CA-ECDH-AES-CBC-CMAC-192 OBJECT IDENTIFIER ::= {id-CA-ECDH 3}
id-CA-ECDH-AES-CBC-CMAC-256 OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

9.2.8 TerminalAuthenticationInfo

This data structure provides detailed information on an implementation of Terminal Authentication.

- The object identifier `protocol` SHALL identify the *general* Terminal Authentication Protocol as the specific protocol may change over time.

- The integer `version` SHALL identify the version of the protocol. Currently, version 1 is supported by this specification. Note that later versions of [TR-03110] define version 2 of this protocol, which is out of scope of this specification.

```
TerminalAuthenticationInfo ::= SEQUENCE {
  protocol OBJECT IDENTIFIER(id-TA),
  version  INTEGER        -- MUST be 1
}
```

9.2.9 Terminal Authentication Object Identifiers

The following Object Identifier SHALL be used:

```
id-TA OBJECT IDENTIFIER ::= {
  bsi-de protocols(2) smartcard(2) 2
}

id-TA-RSA               OBJECT IDENTIFIER ::= {id-TA 1}
id-TA-RSA-PSS-SHA-256   OBJECT IDENTIFIER ::= {id-TA-RSA 4}
id-TA-RSA-PSS-SHA-512   OBJECT IDENTIFIER ::= {id-TA-RSA 6}

id-TA-ECDSA             OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-224     OBJECT IDENTIFIER ::= {id-TA-ECDSA 2}
id-TA-ECDSA-SHA-256     OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384     OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512     OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

9.2.10 EFDIRInfo

This data structure encapsulates a full copy of the content of the transparent elementary file EF.DIR contained in the master file.

```
  EFDIRInfo ::= SEQUENCE {
      protocol                      OBJECT IDENTIFIER(id-EFDIR),
      eFDIR                         OCTET STRING
  }

id-EFDIR OBJECT IDENTIFIER ::={
  id-icao-mrtd-security 13
}
```

9.2.11 Storage on the Chip

To indicate support for the protocols and supported parameters, the eMRTD chip SHALL provide `SecurityInfos` in transparent elementary files (The generic structure of these files can be found in Doc 9303-10):

- The file EF.CardAccess contained in the master file is REQUIRED if PACE is supported by the eMRTD chip and SHALL contain the relevant `SecurityInfos` that are required for PACE:
  - `PACEInfo`
  - `PACEDomainParameterInfo`
- The file EF.CardSecurity contained in the master file is REQUIRED if
  - PACE with Chip Authentication Mapping is supported by the eMRTD chip, or
  - Terminal Authentication in the Master File is supported by the eMRTD chip, or
  - Chip Authentication in the Master File is supported by the eMRTD chip

  and SHALL contain the following `SecurityInfos`:
  - `ChipAuthenticationInfo` as required by Chip Authentication
  - `ChipAuthenticationPublicKeyInfo` as required for PACE-CAM/Chip Authentication
  - `TermninalAuthenticationInfo` as required by Terminal Authentication
  - `EFDIRInfo` if more than the eMRTD Application is present on the chip
  - The `SecurityInfos` contained in EF.CardAccess.
- The file EF.DG14 contained in the eMRTD Application is REQUIRED if
  - PACE with Generic/Integrated Mapping is supported by the eMRTD chip
  - Terminal Authentication in the eMRTD Application is supported by the eMRTD chip, or
  - Chip Authentication in the eMRTD Application is supported by the eMRTD chip

  and SHALL contain the following `SecurityInfos`:
  - `ChipAuthenticationInfo` as required for Chip Authentication
  - `ChipAuthenticationPublicKeyInfo` as required for Chip Authentication
  - `TermninalAuthenticationInfo` as required by Terminal Authentication
  - The `SecurityInfos` contained in EF.CardAccess.
- The full set of `SecurityInfos` (including `SecurityInfos` contained in EF.CardAccess not specified in Doc 9303) SHALL additionally be stored in EF.DG14 of the eMRTD Application (see Doc 9303-10).

The files MAY contain additional `SecurityInfos` out of scope of this specification.

Note.— While the authenticity of `SecurityInfos` *stored in EF.DG14 and EF.CardSecurity is protected*

by Passive Authentication, the file EF.CardAccess is unprotected.

9.3 APDUs

9.3.1 Extended Length

Depending on the size of the cryptographic objects (e.g. public keys, signatures), APDUs with extended length fields MUST be used to send this data to the eMRTD chip. For details on extended length see [ISO/IEC 7816-4].

9.3.1.1 eMRTD Chips

For eMRTD chips, support of extended length is CONDITIONAL. If the cryptographic algorithms and key sizes selected by the issuing State require the use of extended length, the eMRTD chips SHALL support extended length. If the eMRTD chip supports extended length, this MUST be indicated in the ATR/ATS or in EF.ATR/INFO as specified in [ISO/IEC 7816-4].

9.3.1.2 Terminals

For terminals, support of extended length is REQUIRED. A terminal SHOULD examine whether or not support for extended length is indicated in the eMRTD chip's ATR/ATS or in EF.ATR/INFO before using this option. The terminal MUST NOT use extended length for APDUs other than the following commands unless the exact input and output buffer sizes of the eMRTD chip are explicitly stated in the ATR/ATS or in EF.ATR/INFO.

- MSE:Set KAT
- GENERAL AUTHENTICATE

9.3.2 Command Chaining

Command chaining MUST be used for the GENERAL AUTHENTICATE command to link the sequence of commands to the execution of the PACE protocol. Command chaining MUST NOT be used for other purposes unless clearly indicated by the chip. For details on command chaining see [ISO/IEC 7816-4].

9.3.3 Data Objects

The sender of a command or response APDU MUST transmit the data objects in the data field in the order as defined in the APDU descriptions.

Note.— Accepting data objects in any order is not required, but enhances interoperability for some commands, e.g for MSE:Set AT/GENERAL AUTHENTICATE. But care is to be taken in case of commands such as PSO:Verify Certifcate, where the ordering is fixed for cryptographic reasons.

9.4 Public Key Data Objects

A public key data object is a constructed BER TLV structure containing an object identifier and several context specific data objects nested within the cardholder public key template 0x7F49.

- The object identifier is application specific and refers not only to the public key format (i.e. the context

specific data objects) but also to its usage.

- The context-specific data objects are defined by the object identifier and contain the public key value and the domain parameters.

The format of public keys data objects used in this specification is described below.

9.4.1 Data Object Encoding

An unsigned integer SHALL be converted to an octet string using the binary representation of the integer in big-endian format. The minimum number of octets SHALL be used, i.e. leading octets of value 0x00 MUST NOT be used.

To encode elliptic curve points, uncompressed encoding according to [TR-03111] SHALL be used.

9.4.2 RSA Public Keys

Table 9. RSA Public Key

Data Object	Notation	Tag	Type	CV Certificate
Object Identifier		0x06	Object Identifier	m
Composite modulus	*n*	0x81	Unsigned Integer	m
Public exponent	*e*	0x82	Unsigned Integer	m

The data objects contained in an RSA public key are shown in Table 9. The order of the data objects is fixed.

9.4.3 Diffie Hellman Public Keys

The data objects contained in a DH public key are shown in Table 10. The order of the data objects is fixed.

Table 10. Data objects for DH public keys

Data Object	**Notation**	**Tag**	**Type**
Object Identifier		0x06	Object Identifier
Prime modulus	p	0x81	Unsigned Integer
Order of the subgroup	q	0x82	Unsigned Integer
Generator	g	0x83	Unsigned Integer
Public Value	y	0x84	Unsigned Integer

Note.— The encoding of key components as unsigned integer implies that each of them is encoded over the least number of bytes possible, i.e. without preceding bytes set to 0x00. In particular, DH public key may be encoded over a number of bytes smaller than the number of bytes of the prime.

9.4.4 Elliptic Curve Public Keys

The data objects contained in an EC public key are shown in Table 11. The order of the data objects is fixed, CONDITIONAL domain parameters MUST be either all present, except the cofactor, or all absent as follows:

Table 11. Data objects for ECDH public keys

Data Object	Notation	Tag	Type
Object Identifier		0x06	Object Identifier
Prime modulus	p	0x81	Unsigned Integer
First coefficient	a	0x82	Unsigned Integer
Second coefficient	b	0x83	Unsigned Integer
Base point	G	0x84	Elliptic Curve Point
Order of the base point	r	0x85	Unsigned Integer
Public point	Y	0x86	Elliptic Curve Point
Cofactor	f	0x87	Unsigned Integer

9.4.5 Ephemeral Public Keys

For ephemeral public keys the format and the domain parameters are already known. Therefore, only the plain public key value, i.e. the public value y for Diffie-Hellman public keys and the public point Y for Elliptic Curve Public Keys, is used to convey the ephemeral public key in a context specific data object.

Note.— The validation of ephemeral public keys is RECOMMENDED. For DH, the validation algorithm requires the eMRTD chip to have a more detailed knowledge of the domain parameters (i.e. the order of the used subgroup) than usually provided by PKCS#3.

9.5 Domain Parameters

With the exception of domain parameters contained in `PACEInfo`, all domain parameters SHALL be provided as `AlgorithmIdentifier` (cf. Section 9.1).

Within `PACEInfo`, the ID of standardized domain parameters described in Table 12 SHALL be referenced directly. Explicit domain parameters provided by `PACEDomainParameterInfo` MUST NOT use those IDs reserved for standardized domain parameters.

9.5.1 Standardized Domain Parameters

The standardized domain parameters IDs described in the table below SHOULD be used. Explicit domain parameters MUST NOT use those IDs reserved for standardized domain parameters.

The following object identifier SHOULD be used to reference standardized domain parameters in an `AlgorithmIdentifier` (cf. Section 9.1):

```
standardizedDomainParameters OBJECT IDENTIFIER ::= {
  bsi-de algorithms(1) 2
}
```

Within an `AlgorithmIdentifier` this object identifier SHALL reference the ID of the standardized domain parameter as contained in Tableas `INTEGER`, contained as `parameters` in the `AlgorithmIdentifier`.

Table 12. Standardized domain parameters

ID	*Name*	*Size (bit)*	*Type*	*Reference*
0	1024-bit MODP Group with 160-bit Prime Order Subgroup	1024/160	GFP	[RFC 5114]
1	2048-bit MODP Group with 224-bit Prime Order Subgroup	2048/224	GFP	[RFC 5114]
2	2048-bit MODP Group with 256-bit Prime Order Subgroup	2048/256	GFP	[RFC 5114]
3-7	RFU			
8	NIST P-192 (secp192r1)	192	ECP	[RFC 5114], [FIPS 186-4]
9	BrainpoolP192r1	192	ECP	[RFC 5639]
10	NIST P-224 (secp224r1) *	224	ECP	[RFC 5114], [FIPS 186-4]
11	BrainpoolP224r1	224	ECP	[RFC 5639]
12	NIST P-256 (secp256r1)	256	ECP	[RFC 5114], [FIPS 186-4]
13	BrainpoolP256r1	256	ECP	[RFC 5639]
14	BrainpoolP320r1	320	ECP	[RFC 5639]
15	NIST P-384 (secp384r1)	384	ECP	[RFC 5114], [FIPS 186-4]
16	BrainpoolP384r1	384	ECP	[RFC 5639]
17	BrainpoolP512r1	512	ECP	[RFC 5639]
18	NIST P-521 (secp521r1)	521	ECP	[RFC 5114], [FIPS 186-4]
19-31	RFU			

* This curve cannot be used with the Integrated Mapping.

9.5.2 Explicit Domain Parameters

The object identifier `dhpublicnumber` or `ecPublicKey` for DH or ECDH, respectively, SHALL be used to reference explicit domain parameters in an `AlgorithmIdentifier` (cf. Section 9.1):

```
dhpublicnumber OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1
}

ecPublicKey OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) 1
}
```

In the case of elliptic curves, domain parameters MUST be described explicitly in the `ECParameters` structure, contained as `parameters` in the `AlgorithmIdentifier`, i.e. named curves and implicit domain parameters MUST NOT be used.

9.6 Key Agreement Algorithms

This specification supports Diffie-Hellman and Elliptic Curve Diffie-Hellman key agreement as summarized in the following table:

Table 13. Key agreement algorithms

Algorithm / Format	***DH***	***ECDH***
Key Agreement Algorithm	[PKCS#3]	ECKA [TR-03111]
X.509 Public Key Format	[X9.42]	[TR-03111]
TLV Public Key Format	TLV, cf. Section 9.4.2	TLV, cf. Section 9.4.3
Ephemeral Public Key Validation	[RFC 2631]	[TR-03111]

9.7 Key Derivation Mechanism

9.7.1 Key Derivation Function

The key derivation function **KDF**(K,c), is defined as follows:

Input: The following inputs are required:

- The shared secret value K (REQUIRED)
- A 32-bit, big-endian integer counter c (REQUIRED)

Output: An octet string keydata.
Actions: The following actions are performed:

- keydata = **H**(K || c)

- Output octet string keydata

The key derivation function **KDF**(K,c) requires a suitable hash function denoted by **H**(), i.e the bit-length of the hash function SHALL be greater or equal to the bit-length of the derived key. The hash value SHALL be interpreted as big-endian byte output.

Note.— The shared secret K is defined as an octet string. If the shared secret is generated with ECKA [TR-03111], the x-coordinate of the generated point SHALL be used.

9.7.1.1 3DES

To derive 128-bit (112-bit excluding parity bits) 3DES [FIPS 46-3] keys the hash function SHA-1 [FIPS 180-4] SHALL be used and the following additional steps MUST be performed:

- Use octets 1 to 8 of keydata to form keydataA and octets 9 to 16 of keydata to form keydataB; additional octets are not used.

- Adjust the parity bits of keydataA and keydataB to form correct DES keys (OPTIONAL).

9.7.1.2 AES

To derive 128-bit AES [FIPS 197] keys the hash function SHA-1 [FIPS 180-4] SHALL be used and the following additional step MUST be performed:

- Use octets 1 to 16 of keydata; additional octets are not used.

To derive 192-bit and 256-bit AES [FIPS 197] keys SHA-256 [FIPS 180-4] SHALL be used. For 192-bit AES keys the following additional step MUST be performed:

- Use octets 1 to 24 of keydata; additional octets are not used.

9.7.2 Document Basic Access Keys

The computation of two key 3DES keys from a key seed (K) is used in the establishment of the Document Basic Access Keys K_{Enc} = **KDF**(K,1) and K_{MAC} = **KDF**(K,2).

9.7.3 PACE

Let $\mathbf{KDF}_{\pi}(\pi)$ = **KDF**(f(π),3) be a key derivation function to derive encryption keys from a password π. The encoding of passwords, i.e. K= f(π) is specified in Table 14:

Table 14. Password encodings

Password	Encoding
MRZ	SHA-1(Document Number || Date of Birth || Date of Expiry)

CAN	[ISO/IEC 8859-1] encoded character string

Note.— The document number to be used as input is always the complete document number. In case of TD1-documents with document numbers longer than 9 characters, the document number needs to be concatenated from the document number field and the optional data field of the MRZ, excluding the filler character. See also note j in Section 4.2.2 in Doc 9303-5,

9.7.4 Secure Messaging Keys

Keys for encryption and authentication are derived with $\mathbf{KDF}_{Enc}(K) = \mathbf{KDF}(K,1)$ and $\mathbf{KDF}_{MAC}(K) = \mathbf{KDF}(K,2)$ respectively, from a shared secret K.

9.8 Secure Messaging

9.8.1 Session Initiation

A session is started when secure messaging is established. Within a session the secure messaging keys (i.e. established by Basic Access Control, PACE or Chip Authentication) may be changed.

Secure Messaging is based on either 3DES [FIPS 46-3] or AES [FIPS 197] in encrypt-then-authenticate mode, i.e. data is padded, encrypted and afterwards the formatted encrypted data is input to the authentication calculation. The session keys SHALL be derived using the key derivation function described in Section 9.7.1.

Note.— Padding is always performed by the secure messaging layer, therefore the underlying message authentication code need not perform any internal padding.

9.8.2 Send Sequence Counter

An unsigned integer SHALL be used as Send Sequence Counter (SSC). The bitsize of the SSC SHALL be equal to the blocksize of the block cipher used for Secure Messaging, i.e., 64 bit for 3DES and 128 bit for AES.

The SSC SHALL be increased every time before a command or response APDU is generated, i.e., if the starting value is x, in the first command the value of the SSC is x+1. The value of SSC for the first response is x+2.

If Secure Messaging is restarted, the SSC is used as follows:

- The commands used for key agreement are protected with the old session keys and old SSC. This applies in particular for the response of the last command used for session key agreement.
- The Send Sequence Counter is set to its new start value, see Section 9.8.6.3 for 3DES/ Section 9.8.7.3 for AES.
- The new session keys and the new SSC are used to protect subsequent commands/responses.

9.8.3 Session Termination

The eMRTD chip MUST abort Secure Messaging if and only if a Secure Messaging error occurs or a plain APDU is received.

If Secure Messaging is aborted, the eMRTD chip SHALL delete the stored session keys and reset the terminal's access rights.

Note.— The eMRTD chip MAY implicitly select the Master File when a session is terminated.

9.8.4 Message Structure of SM APDUs

The SM Data Objects (see [ISO/IEC 7816-4]) MUST be used in the following order:

- Command APDU: [DO'85' or DO'87'] [DO'97'] DO'8E'.
- Response APDU: [DO'85' or DO'87'] [DO'99'] DO'8E'.

In case INS is even, DO'87' SHALL be used, and in case INS is odd, DO'85' SHALL be used.

All SM Data Objects MUST be encoded in BER TLV as specified in [ISO/IEC 7816-4]. The command header MUST be included in the MAC calculation, therefore the class byte CLA = 0x0C MUST be used.

The actual value of Lc will be modified to Lc' after application of Secure Messaging. If required, an appropriate data object may optionally be included into the APDU data part in order to convey the original value of Lc.

Figure 5 shows the transformation of an unprotected command APDU to a protected command APDU in the case *Data* and *Le* are available. If no *Data* is available, leave building DO '87' out. If *Le* is not available, leave building DO '97' out. To avoid ambiguity it is RECOMMENDED not to use an empty value field of Le Data Object (see also Section 10.4 of [ISO/IEC 7816-4]).

Figure 6 shows the transformation of an unprotected response APDU to a protected response APDU in case *Data* is available. If no *Data* is available, leave building DO '87' out.

9.8.5 SM Errors

Abortion of the Secure Channel for the eMRTD Application occurs when:

- the contactless IC is de-powered; or
- the contactless IC recognizes an SM error while interpreting a command. In this case the status bytes must be returned without SM.

If Secure Messaging is aborted, the eMRTD chip SHALL delete the stored session keys and reset the terminal's access rights.

Note.— There MAY be other circumstances in which the contactless IC aborts the session. It is not feasible to provide a complete list of such circumstances.

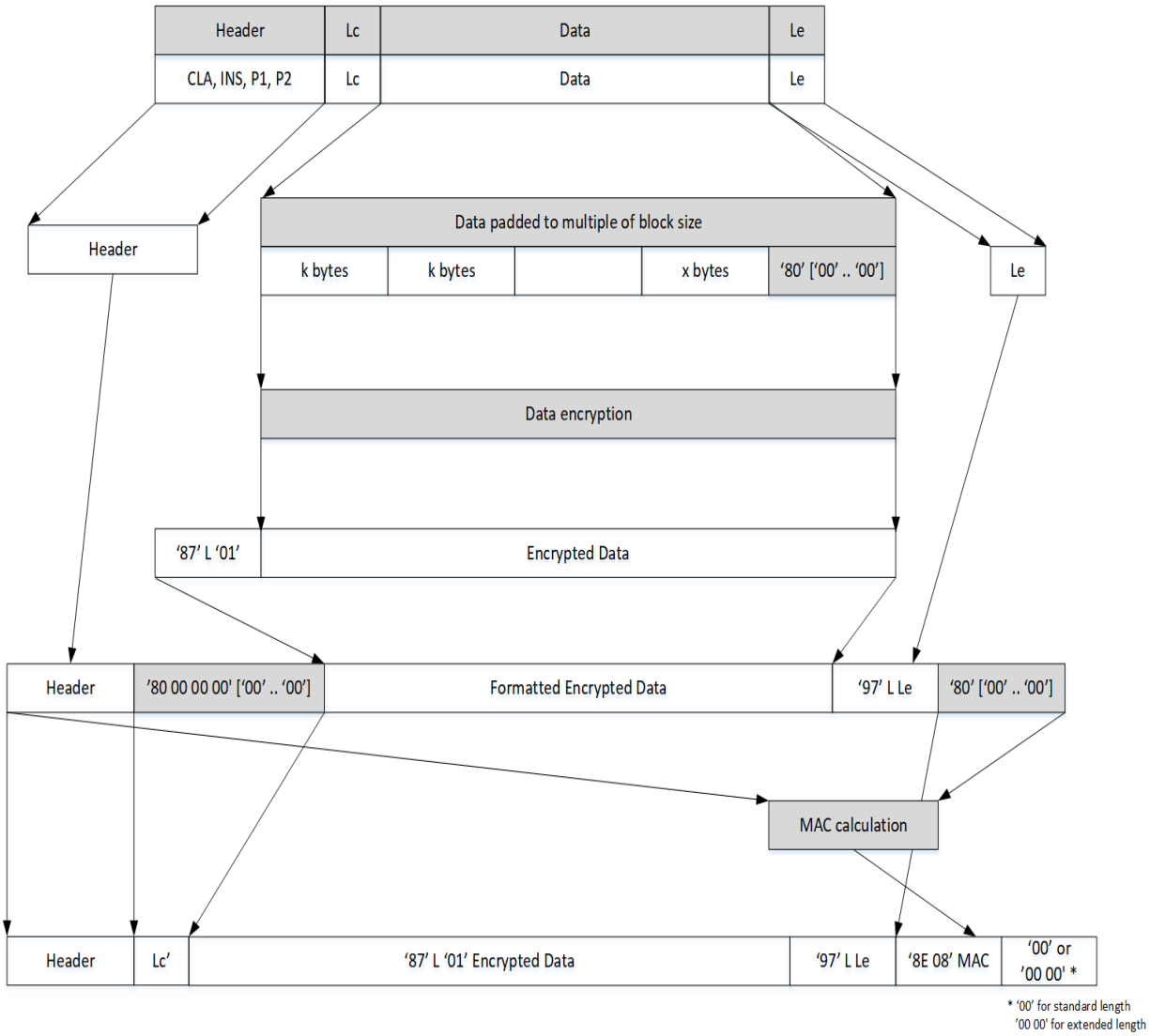


Figure 5. Computation of an SM command APDU for even INS Byte

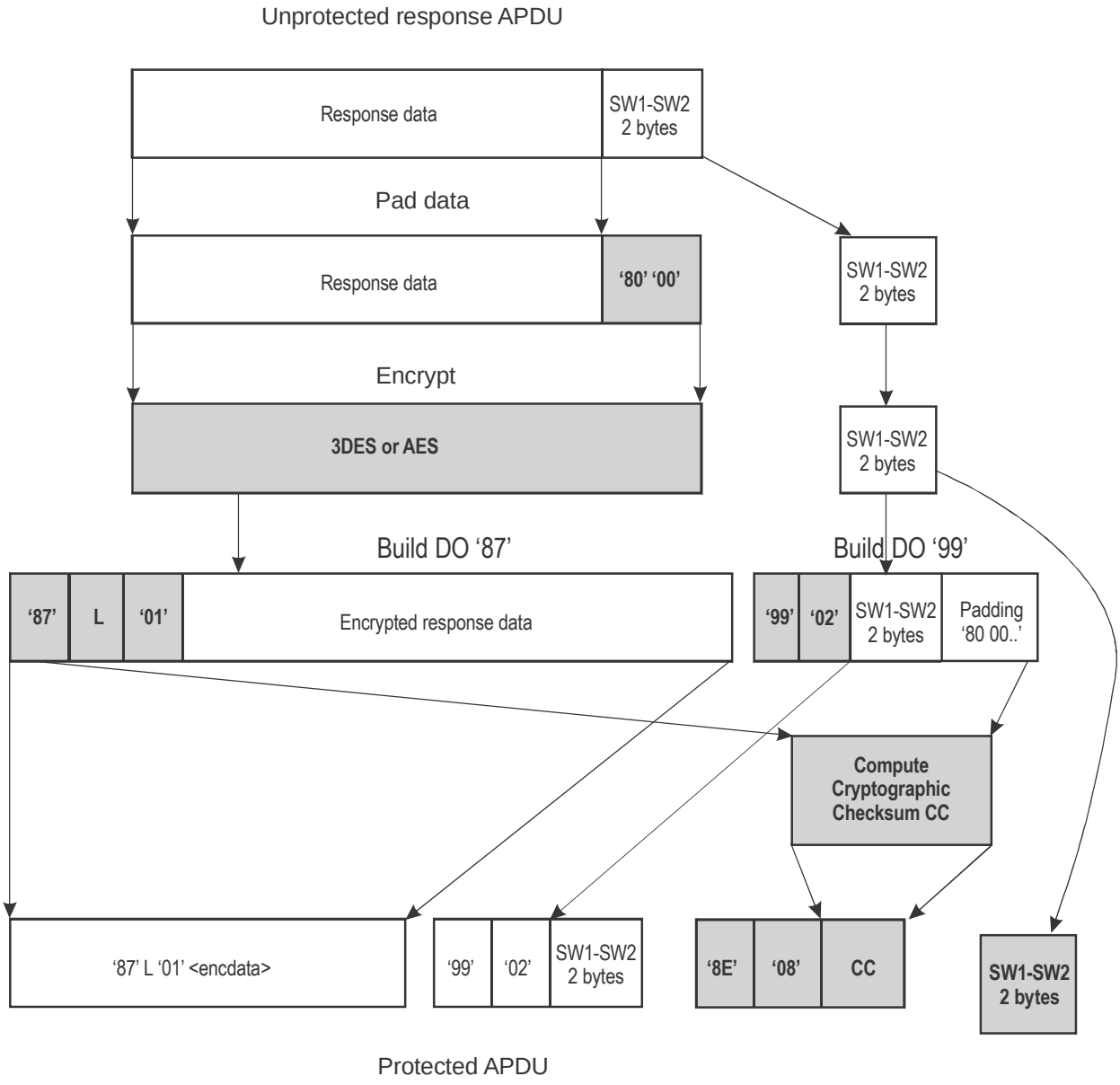


Figure 6. Computation of an SM response APDU for even INS Byte

9.8.6 3DES Modes of Operation

9.8.6.1 Encryption

Two key 3DES in CBC mode with zero IV (i.e. 0x00 00 00 00 00 00 00 00) according to [ISO/IEC 11568-2] is used. Padding according to [ISO/IEC 9797-1] padding method 2 is used.

9.8.6.2 Message Authentication

Cryptographic checksums are calculated using [ISO/IEC 9797-1] MAC algorithm 3 with block cipher DES, zero IV (8 bytes), and [ISO/IEC 9797-1] padding method 2. The MAC length MUST be 8 bytes.

After a successful authentication the datagram to be MACed MUST be prepended by the Send Sequence Counter.

9.8.6.3 Send Sequence Counter

For Secure Messaging following BAC, the Send Sequence Counter SHALL be initialized by concatenating the four least significant bytes of RND.IC and RND.IFD, respectively:

SSC = RND.IC (4 least significant bytes) || RND.IFD (4 least significant bytes).

In all other cases, the SSC SHALL be initialized to zero (i.e. 0x00 00 00 00 00 00 00 00).

9.8.7 AES Modes of Operation

9.8.7.1 Encryption

For message encryption AES [FIPS 197] SHALL be used in CBC-mode according to [ISO/IEC 10116] with key KS_{Enc} and IV = **E**(KS_{Enc}, SSC).

9.8.7.2 Message Authentication

For message authentication AES SHALL be used in CMAC-mode [SP 800-38B] with KS_{MAC} with a MAC length of 8 bytes. The datagram to be authenticated SHALL be prepended by the Send Sequence Counter.

9.8.7.3 Send Sequence Counter

The Send Sequence Counter SHALL be initialized to zero (i.e. 0x00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00).

10. REFERENCES (NORMATIVE)

[X9.42]	ANSI: X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 1999
[ISO/IEC 7816-4]	ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange
[ISO/IEC 7816-8]	ISO/IEC 7816-8:2019 Identification cards — Integrated circuit cards — Part 8: Commands for security operations
[ISO/IEC 8859-1]	ISO/IEC 8859-1:1998 Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1
[ISO/IEC 9796-2]	ISO/IEC 9796-2:2010 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
[ISO/IEC 9797-1]	ISO/IEC 9797-1:2011 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
[ISO/IEC 10116]	ISO/IEC 10116:2017 Information technology − Security techniques − Modes of operation for an n-bit block cipher
[ISO/IEC 11568-2]	ISO/IEC 11568-2:2012 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle
[ISO/IEC 11770-2]	ISO/IEC 11770-2:2018 Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques
[FIPS 46-3]	NIST FIPS PUB 46-3, Data Encryption Standard (DES), 1999
[FIPS 180-4]	NIST FIPS PUB 180-4, Secure hash standard, 2015
[FIPS 186-4]	NIST FIPS PUB 186-4, Digital Signature Standard (DSS), 2013
[FIPS 197]	NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), 2001
[SP 800-38B]	NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
[RFC 2631]	Rescorla, Eric: RFC 2631 Diffie-Hellman key agreement method, 1999
[RFC 3447]	Jonsson, Jakob and Kaliski, Burt: RFC 3447, Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1, 2003
[RFC 5114]	Lepinski, Matt; Kent, Stephen: RFC 5114 Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
[RFC 5280]	D. Cooper, S. Santesson, S. Farrell, S. Boyen, R. Housley, W. Polk, RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008
[RFC 5639]	Lochter, Manfred; Merkle, Johannes: RFC 5639 Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010
[TR-03110]	BSI: Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents
[TR-03111]	BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2012
[PKCS#1]	RSA Laboratories, PKCS#1 v2.1: RSA cryptography standard, 2002
[PKCS#3]	RSA Laboratories, PKCS#3: Diffie-Hellman key-agreement standard, 1993
[Keesing2009]	J. Bender, D. Kügler: Introducing the PACE solution, in: Keesing Journal of Documents & Identity, Issue 30, Keesing, 2009.
[BFK2009]	J. Bender, M. Fischlin, D. Kügler: Security Analysis of the PACE Key-Agreement Protocol, in: Proceedings ISC 2009, LNCS volume 5735, Springer, 2009.
[BCIMRT2010]	Brier, Eric; Coron, Jean-Sébastien; Icart, Thomas; Madore, David; Randriam, Hugues; and Tibouch, Mehdi, Efficient Indifferentiable Hashing into Ordinary Elliptic Curves, Advances in Cryptology – CRYPTO 2010, Springer-Verlag, 2010

— — — — — — — —

Appendix A to Part 11

ENTROPY OF MRZ-DERIVED ACCESS KEYS (INFORMATIVE)

Due to its simplicity Basic Access Control turned out to be a very successful protocol and it is implemented in almost every eMRP.

The security provided by Basic Access Control is limited by the design of the protocol. The Document Basic Access Keys (K_{Enc} and K_{MAC}) are generated from printed data with very limited randomness. The data that is used for the generation of the keys are Document Number, Date of Birth, and Date of Expiry. As a consequence the resulting keys have a relatively low entropy and are cryptographically weak. The actual entropy mainly depends on the type of the Document Number. For a 10-year valid travel document the maximum strength of the keys is approximately:

- 56 Bit for a numeric Document Number ($365^2 * 10^{12}$ possibilities)
- 73 Bit for an alphanumeric Document Number ($365^2*36^9*10^3$ possibilities).

Especially in the second case this estimation requires the Document Number to be randomly and uniformly chosen which is usually not the case. Depending on the knowledge of the attacker, the actual entropy of the Document Basic Access Key may be lower, e.g. if the attacker knows all Document Numbers in use or is able to correlate Document Numbers and Dates of Expiry.

There is no straightforward way to strengthen Basic Access Control as its limitations are inherent to the design of the protocol based on symmetric (“secret key”) cryptography. A cryptographically strong access control mechanism must (additionally) use asymmetric (“public key”) cryptography.

Password Authenticated Connection Establishment (PACE) was designed to overcome this problem. It employs asymmetric cryptography to establish session keys, whose strength is independent of the entropy of the used password. If PACE is implemented with elliptic curve cryptography with 256 Bit curves and AES-128 (a common choice), the session keys have 128 Bit entropy.

Two types of attacks must be distinguished:

- Skimming: this is an online attack, i.e. the attacker tries to access the contactless IC in real time, e.g. by guessing the password. If the protocol used to protect the contactless IC has no cryptographic weakness, the success probability of the attacker is given by the time the attacker has access to the IC, the duration of a single attempt to guess the password, and the entropy of the passport.
- Eavesdropping: this is an offline attack, i.e. the attacker tries to decrypt intercepted communication without access to the contactless IC. If the protocol used to establish the session keys has no cryptographic weakness, the success probability is given by the strength of the session keys and the computing power available to the attacker.

For further information see [Keesing2009] for a general discussion on entropy of session keys and a comparison of BAC and PACE, and [BFK2009] for a cryptographic analysis of PACE.

— — — — — — — —

Appendix B to Part 11

POINT ENCODING FOR THE ECDH-INTEGRATED MAPPING (INFORMATIVE)

B.1 HIGH-LEVEL DESCRIPTION OF THE POINT ENCODING METHOD

The algorithm takes as inputs the curve parameters (a, b, p, f) where (a, b) are the curve coefficients, p is the characteristic of the prime field over which the curve

$$E : y^2 \equiv x^3 + ax + b \ (mod\ p)$$

is defined. The order of E is always of the form fq for some prime q and f is called the co-factor. PACE v2 requires the generation of a point that belongs to the q-subgroup of E that we denote by $E[q]$. The point encoding also takes as input a number t such that

$$0 < t < p$$

and returns, in constant time, a point that belongs to $E[q]$. As described in [BCIMRT2010], point encoding comes in two flavours, depending on the coordinate system preferred by the implementation:

- A first implementation, described in Section B.2, outputs the elliptic curve point in affine coordinates (x, y);
- An alternate implementation, presented in Section B.3, outputs the same point in Jacobian coordinates (X, Y, Z).

Irrespective of the option taken, the generated point is identical in the sense that

$$x = XZ^{-2} \ mod\ p \ and \ y = YZ^{-3} \ mod\ p$$

and the implementation of the subsequent phase of PACE v2 (the elliptic curve Diffie-Hellman key exchange phase) can therefore take advantage of using the option that best fits the interface of the cryptographic API that performs elliptic-curve operations.

As noted hereafter, point encoding for affine coordinates roughly requires two modular exponentiations modulo p whereas point encoding for Jacobian coordinates requires only a single one.

Note that for the two available implementations, point encoding explicitly requires that $p \equiv 3 \ mod\ 4$.

B.2 IMPLEMENTATION FOR AFFINE COORDINATES

The algorithm is implemented as follows:
Inputs: curve parameters (a, b, p, f) and t such that $0 < t < p$

Output: a point (x, y) in the prime-order subgroup $E[q]$ of E

1. Compute $\alpha = -t^2 \bmod p$
2. Compute $X_2 = -ba^{-1}(1+(\alpha+\alpha^2)^{-1}) \bmod p$
3. Compute $X_3 = \alpha X_2 \bmod p$
4. Compute $h_2 = (X_2)^3 + a X_2 + b \bmod p$
5. Compute $h_3 = (X_3)^3 + a X_3 + b \bmod p$
6. Compute $U = t^3 h_2 \bmod p$
7. Compute $A = (h_2)^{p-1-(p+1)/4} \bmod p$
8. If $A^2 h_2 = 1 \bmod p$ define $(x, y) = (X_2, A h_2 \bmod p)$
9. Otherwise define $(x, y) = (X_3, A U \bmod p)$
10. Output $(x, y) = [f] (x, y)$.

Implementation Notes

Neglecting modular multiplications and additions, the execution time of the above implementation is dominated by two modular exponentiations:

- Step 2 can be rewritten

$$X_2 = -ba^{-1}(1+(\alpha+\alpha^2)^{-1}) = -b(1+\alpha+\alpha^2)\,(a(\alpha+\alpha^2))^{p-2} \bmod p$$

  which essentially amounts to a modular exponentiation with exponent $p-2$;

- Step 7 is a modular exponentiation with exponent $p-1-(p+1)/4$.

Note.— Step 10 requires a scalar multiplication by the co-factor f. *For many curves, the co-factor is equal to 1 so that this scalar multiplication can be avoided.*

B.3 IMPLEMENTATION FOR JACOBIAN COORDINATES

The algorithm is implemented as follows:

Inputs: curve parameters (a, b, p, f) and t such that $0 < t < p$

Output: a point (X, Y, Z) in the prime-order subgroup $E[q]$ of E

1. Compute $\alpha = -t^2 \bmod p$
2. Compute $Z = a(\alpha+\alpha^2) \bmod p$
3. Compute $X_2 = -bZ\,(1+\alpha+\alpha^2) \bmod p$
4. Compute $X_3 = \alpha X_2 \bmod p$
5. Compute $h_2 = (X_2)^3 + a X_2 Z^4 + b Z^6 \bmod p$
6. Compute $h_3 = (X_3)^3 + a X_3 Z^4 + b Z^6 \bmod p$
7. Compute $U = -\alpha\, t\, h_2 \bmod p$
8. Compute $A = (h_2)^{p-1-(p+1)/4} \bmod p$
9. If $A^2 h_2 = 1 \bmod p$ define $(X, Y, Z) = (X_2, A h_2 \bmod p, Z)$
10. Otherwise define $(X, Y, Z) = (X_3, A U \bmod p, Z)$
11. Output $(X, Y, Z) = [f](X, Y, Z)$.

Implementation Notes

Neglecting modular multiplications and additions, the execution time of the above implementation is dominated by the single modular exponentiation of Step 7. Therefore, it is expected to be roughly twice as fast as the implementation for affine coordinates.

Note.— The scalar multiplication in Step 10 can be completely avoided when the co-factor f *is equal to 1.*

— — — — — — — —

Appendix C to Part 11

CHALLENGE SEMANTICS (INFORMATIVE)

Consider a signature based challenge-response protocol between an eMRTD chip (IC) and a terminal (IFD), where the eMRTD chip wants to prove knowledge of its private key SK_{IC}:

- The terminal sends a randomly chosen challenge *c* to the eMRTD chip.
- The eMRTD chip responds with the signature *s*=**Sign**(SK_{IC},c).

While this is a very simple and efficient protocol, the eMRTD chip in fact signs the message *c* without knowing the semantic of this message. As signatures provide a transferable proof of authenticity, any third party can – in principle – be convinced that the eMRTD chip has indeed signed this message.

Although *c* should be a random bit string, the terminal can as well generate this bit string in an unpredictable but (publicly) verifiable way, e.g., let SK_{IFD} be the terminal's private key and

$$c = \textbf{Sign}(SK_{IFD}, ID_{IC} || Date || Time || Location)$$

be the challenge generated by using a signature scheme with message recovery. The signature guarantees that the terminal has indeed generated this challenge. Due to the transferability of the terminal's signature, any third party having trust in the terminal and knowing the corresponding public key PK_{IFD} can check that the challenge was created correctly by verifying this signature. Furthermore, due to the transferability of eMRTD chip's signature on the challenge, the third party can conclude that the assertion became true: The eMRTD chip was indeed at a certain date and time at a certain location.

On the positive side, States may use Challenge Semantics for their internal use, e.g., to prove that a certain person indeed has immigrated. On the negative side such proofs can be misused to track persons. In particular since Active Authentication is not restricted to authorized terminals, misuse is possible. The worst scenario would be eMRTD chips that provide Active Authentication without Basic Access Control. In this case a very powerful tracking system may be set up by placing secure hardware modules at prominent places. The resulting logs cannot be faked due to the signatures. Basic Access Control diminishes this problem to a certain extent, as interaction with the bearer is required. Nevertheless, the problem remains, but is restricted to places where the travel document of the bearer is read anyway, e.g., by airlines or hotels.

One might object that especially in a contactless scenario, challenges may be eavesdropped and reused at a different date, time or location and thus render the proof at least unreliable. While eavesdropping challenges are technically possible, the argument is still invalid. By assumption a terminal is trusted to produce challenges correctly, and it can be assumed that it has checked the eMRTD chip's identity before starting Active Authentication. Thus, the eavesdropped challenge will contain an identity different from the identity of the prover who signs the challenge.

— — — — — — — —

Appendix D to Part 11

WORKED EXAMPLE: BASIC ACCESS CONTROL (INFORMATIVE)

D.1 COMPUTE KEYS FROM KEY SEED (K_{SEED})

This Section provides an example for derivation of 3DES keys from a seed value K_{seed}. This procedure will be used as a "subroutine" in the examples for Basic Access Control.

Input:

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

Compute encryption key (c = '00000001'):

1. Concatenate K_{seed} and c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000001'

2. Calculate the SHA-1 hash of D:
   H_{SHA-1}(D) = 'AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D'

3. Form DES keys K_a and K_b, intended to be used as first and second key for 3DES (i.e. the 3DES key is the concatenation of K_a and K_b):
   $K_{a'}$ = 'AB94FCEDF2664EDF'
   $K_{b'}$ = 'B9B291F85D7F77F2'

4. Adjust parity bits:
   K_a = 'AB94FDECF2674FDF'
   K_b = 'B9B391F85D7F76F2'

Compute MAC computation key (c = '00000002'):

1. Concatenate K_{seed} and c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000002'

2. Calculate the SHA-1 hash of D:
   H_{SHA-1}(D) = '7862D9ECE03C1BCD4D77089DCF131442814EA70A'

3. Form keys $K_{a'}$ and $K_{b'}$:
   $K_{a'}$ = '7862D9ECE03C1BCD'
   $K_{b'}$ = '4D77089DCF131442'

4. Adjust parity bits:
   K_a = '7962D9ECE03D1ACD'
   K_b = '4C76089DCE131543'

D.2 DERIVATION OF DOCUMENT BASIC ACCESS KEYS (K_{ENC} AND K_{MAC})

This section provides examples how the Basic Access Keys are derived from the MRZ.

TD2 MRZ, document number exceeds 9 characters

1. Read the MRZ

   MRZ = `I<UTOSTEVENSON<<PETER<JOHN<<<<<<<<<<`
   `D23145890<UTO3407127M95071227349<<<8`

2. Construct the 'MRZ information' from the MRZ

   Document number = `D23145890734` check digit = `9`
   Date of Birth = `340712` check digit = `7`
   Date of Expiry = `950712` check digit = `2`
   MRZ_information = `D23145890734934071279507122`

Continue with step 3.

TD2 MRZ, document number 9 characters

1. Read the MRZ:

   MRZ = `I<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<`
   `L898902C<3UTO6908061F9406236<<<<<<<8`

2. Construct the 'MRZ_information' from the MRZ:

   Document number = `L898902C<` check digit = `3`
   Date of birth = `690806` check digit = `1`
   Date of expiry = `940623` check digit = `6`
   MRZ_information = `L898902C<3690806194062 36`

Continue with step 3.

TD1 MRZ, document number exceeds 9 characters

1. Read the MRZ

   MRZ = `I<UTOD23145890<7349<<<<<<<<<<`
   `3407127M9507122UTO<<<<<<<<<<<2`
   `STEVENSON<<PETER<JOHN<<<<<<<<<`

2. Construct the 'MRZ information' from the MRZ

   Document number = `D23145890734` check digit = `9`
   Date of Birth = `340712` check digit = `7`
   Date of Expiry = `950712` check digit = `2`
   MRZ_information = `D23145890734934071279507122`

Continue with step 3.

TD1 MRZ, document number 9 characters

1. Read the MRZ

   MRZ = `I<UTOL898902C<3<<<<<<<<<<<<<<`
   `6908061F9406236UTO<<<<<<<<<<<1`
   `ERIKSSON<<ANNA<MARIA<<<<<<<<<<`

2. Construct the 'MRZ information' from the MRZ

Document number	= L898902C<	check digit = 3
Date of Birth	= 690806	check digit = 1
Date of Expiry	= 940623	check digit = 6
MRZ_information	= L898902C<3690806194062 36	

3. Calculate the SHA-1 hash of 'MRZ_information':
H_{SHA-1}(MRZ_information) = '239AB9CB282DAF66231DC5A4DF6BFBAEDF477565'

4. Take the most significant 16 bytes to form the K_{seed}:
K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

5. Calculate the basic access keys (K_{Enc} and K_{MAC}) according to Section 9.7.1/Appendix D.1:
K_{Enc} = 'AB94FDECF2674FDFB9B391F85D7F76F2'
K_{MAC} = '7962D9ECE03D1ACD4C76089DCE131543'

D.3 AUTHENTICATION AND ESTABLISHMENT OF SESSION KEYS

This section provides an example for performing Basic Access Control.

Inspection system:

1. Request an 8 byte random number from the eMRTD's contactless IC:

Command APDU:				
CLA	**INS**	**P1**	**P2**	**Le**
00	84	00	00	08

Response APDU:	
Response data field	**SW1-SW2**
RND.IC	9000

RND.IC = '4608F91988702212'

2. Generate an 8 byte random and a 16 byte random:
RND.IFD = '781723860C06C226'
K_{IFD} = '0B795240CB7049B01C19B33E32804F0B'

3. Concatenate RND.IFD, RND.IC and K_{IFD}:
S = '781723860C06C2264608F91988702212
0B795240CB7049B01C19B33E32804F0B'

4. Encrypt S with 3DES key K_{Enc}:
E_{IFD} = '72C29C2371CC9BDB65B779B8E8D37B29
ECC154AA56A8799FAE2F498F76ED92F2'

5. Compute MAC over E_{IFD} with 3DES key K_{MAC}:
   M_{IFD} = '5F1448EEA8AD90A7'

6. Construct command data for EXTERNAL AUTHENTICATE and send command APDU to the eMRTD's contactless IC:
   cmd_data = '72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
   56A8799FAE2F498F76ED92F25F1448EEA8AD90A7'

Command APDU:						
CLA	**INS**	**P1**	**P2**	**Lc**	**Command data field**	**Le**
00	82	00	00	28	cmd_data	28

eMRTD's contactless IC:

1. Decrypt and verify received data and compare RND.IC with response on GET CHALLENGE.

2. Generate a 16 byte random:
   K_{IC} = '0B4F80323EB3191CB04970CB4052790B'

3. Calculate XOR of K_{IFD} and K_{IC}:
   K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

4. Calculate session keys (KS_{Enc} and KS_{MAC}) according to Section 9.7.1/Appendix D.1:
   KS_{Enc} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
   KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

5. Calculate send sequence counter:
   SSC = '887022120C06C226'

6. Concatenate RND.IC, RND.IFD and K_{IC}:
   R = '4608F91988702212781723860C06C226
   0B4F80323EB3191CB04970CB4052790B'

7. Encrypt R with 3DES key K_{Enc}:
   E_{IC} = '46B9342A41396CD7386BF5803104D7CE
   DC122B9132139BAF2EEDC94EE178534F'

8. Compute MAC over E_{IC} with 3DES key K_{MAC}:
   M_{IC} = '2F2D235D074D7449'

9. Construct response data for EXTERNAL AUTHENTICATE and send response APDU to the inspection system:
   resp_data = '46B9342A41396CD7386BF5803104D7CEDC122B91
   32139BAF2EEDC94EE178534F2F2D235D074D7449'

Response APDU:	
Response data field	**SW1-SW2**
resp_data	9000

Inspection system:

1. Decrypt and verify received data and compare received RND.IFD with generated RND.IFD.

2. Calculate XOR of K_{IFD} and K_{IC}:
   K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

3. Calculate session keys (KS_{Enc} and KS_{MAC}) according to Section 9.7.1/Appendix D.1:
   KS_{Enc} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
   KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

4. Calculate send sequence counter:
   SSC = '887022120C06C226'

D.4 SECURE MESSAGING

After authentication and establishment of the session keys, the inspection system selects the EF.COM (File ID = '011E') and reads the data using secure messaging. The calculated KS_{Enc}, KS_{MAC} and SSC (previous steps 3 and 4 of the inspection system) will be used.

First the EF.COM will be selected, then the first four bytes of this file will be read so that the length of the structure in the file can be determined and after that the remaining bytes are read.

1. Select EF.COM

   Unprotected command APDU:

CLA	INS	P1	P2	Lc	Command data field
00	A4	02	0C	02	01 1E

   a) Mask class byte and pad command header:
      CmdHeader = '0CA4020C80000000'

   b) Pad data:
      Data = '011E800000000000'

   c) Encrypt data with KS_{Enc}:
      EncryptedData = '6375432908C044F6'

   d) Build DO'87':
      DO87 = '8709016375432908C044F6'

   e) Concatenate CmdHeader and DO'87':
      M = '0CA4020C8000000087090163754329 08C044F6'

f) Compute MAC of M:

i) Increment SSC with 1:

SSC = '887022120C06C227'

ii) Concatenate SSC and M and add padding:

N = '887022120C06C2270CA4020C80000000
8709016375432908C044F68000000000'

iii) Compute MAC over N with KS_{MAC}:

CC = 'BF8B92D635FF24F8'

g) Build DO'8E':

DO8E = '8E08BF8B92D635FF24F8'

h) Construct and send protected APDU:

ProtectedAPDU = '0CA4020C158709016375432908C0
44F68E08BF8B92D635FF24F800'

i) Receive response APDU of eMRTD's contactless IC:

RAPDU = '990290008E08FA855A5D4C50A8ED9000'

j) Verify RAPDU CC by computing MAC of DO'99':

i) Increment SSC with 1:

SSC = '887022120C06C228'

ii) Concatenate SSC and DO'99' and add padding:

K = '887022120C06C2289902900080000000'

iii) Compute MAC with KS_{MAC}:

CC' = 'FA855A5D4C50A8ED'

iv) Compare CC' with data of DO'8E' of RAPDU.

'FA855A5D4C50A8ED' == 'FA855A5D4C50A8ED' ? YES.

2. Read Binary of first four bytes:

Unprotected command APDU:

CLA	INS	P1	P2	Le
00	B0	00	00	04

a) Mask class byte and pad command header:

CmdHeader = '0CB0000080000000'

b) Build DO'97':

DO97 = '970104'

c) Concatenate CmdHeader and DO'97':

M = '0CB000008000000970104'

d) Compute MAC of M:

i) Increment SSC with 1:
SSC = ‘887022120C06C229’

ii) Concatenate SSC and M and add padding:
N = ‘887022120C06C2290CB00000
80000000970104800000000’

iii) Compute MAC over N with KSMAC:
CC = ‘ED6705417E96BA55’

e) Build DO‘8E’:
DO8E = ‘8E08ED6705417E96BA55’

f) Construct and send protected APDU:
ProtectedAPDU = ‘0CB000000D9701048E08ED6705417E96BA5500’

g) Receive response APDU of eMRTD’s contactless IC:
RAPDU = ‘8709019FF0EC34F992265199029000
8E08AD55CC17140B2DED9000’

h) Verify RAPDU CC by computing MAC of concatenation DO‘87’ and DO‘99’:

i) Increment SSC with 1:
SSC = ‘887022120C06C22A’

ii) Concatenate SSC, DO‘87’ and DO‘99’ and add padding:
K = ‘887022120C06C22A8709019F
F0EC34F99226519902900080’

iii) Compute MAC with KS_{MAC}:
CC’ = ‘AD55CC17140B2DED’

iv) Compare CC’ with data of DO‘8E’ of RAPDU:
‘AD55CC17140B2DED’ == ‘AD55CC17140B2DED’ ? YES.

i) Decrypt data of DO‘87’ with KS_{Enc}:
DecryptedData = ‘60145F01’

j) Determine length of structure:
L = ‘14’ + 2 = 22 bytes

3. Read Binary of remaining 18 bytes from offset 4:

Unprotected command APDU:

CLA	INS	P1	P2	Le
00	B0	00	04	12

a) Mask class byte and pad command header:
CmdHeader = ‘0CB0000480000000’

b) Build DO‘97’:
DO97 = ‘970112’

c) Concatenate CmdHeader and DO‘97’:
M = ‘0CB000048000000970112’

d) Compute MAC of M:

i) Increment SSC with 1:
SSC = ‘887022120C06C22B’

ii) Concatenate SSC and M and add padding:
N = ‘887022120C06C22B0CB00004
80000000970112800000000’

iii) Compute MAC over N with KS_{MAC}:
CC = ‘2EA28A70F3C7B535’

e) Build DO‘8E’:
DO8E = ‘8E082EA28A70F3C7B535’

f) Construct and send protected APDU:
ProtectedAPDU = ‘0CB000040D9701128E082EA28A70F3C7B53500’

g) Receive response APDU of eMRTD’s contactless IC:
RAPDU = ‘871901FB9235F4E4037F2327DCC8964F1F9B8C30F42
C8E2FFF224A990290008E08C8B2787EAEA07D749000’

h) Verify RAPDU CC by computing MAC of concatenation DO‘87’ and DO‘99’:

i) Increment SSC with 1:
SSC = ‘887022120C06C22C’

ii) Concatenate SSC, DO‘87’ and DO‘99’ and add padding:
K = ‘887022120C06C22C871901FB9235F4E4037F232
7DCC8964F1F9B8C30F42C8E2FFF224A99029000’

iii) Compute MAC with KS_{MAC}:
CC’ = ‘C8B2787EAEA07D74’

iv) Compare CC’ with data of DO‘8E’ of RAPDU:
‘C8B2787EAEA07D74’ == ‘C8B2787EAEA07D74’ ? YES.

i) Decrypt data of DO‘87’ with KS_{Enc}:
DecryptedData = ‘04303130365F36063034303030305C026175’

RESULT:

EF.COM data = ‘60145F0104303130365F36063034303030305C026175’

— — — — — — — —

Appendix E to Part 11

WORKED EXAMPLE: PASSIVE AUTHENTICATION (INFORMATIVE)

Step 1. Read the Document Security Object (SO_D) (optionally containing the Document Signer Certificate (C_{DS})) from the contactless IC.

Step 2: Read the Document Signer (DS) from the Document Security Object (SO_D).

Step 3: The inspection system verifies SO_D by using Document Signer Public Key.

Step 4: The inspection system verifies C_{DS} by using the Country Signing CA Public Key.

If both verifications in step 3 and 4 are correct, then this ensures that the contents of SO_D can be trusted and can be used in the inspection process.

Step 5: Read the relevant Data Groups from the LDS.

Step 6: Calculate the hashes of the relevant Data Groups.

Step 7: Compare the calculated hashes with the corresponding hash values in the SO_D.

If the hash values in step 7 are identical, this ensures that the contents of the Data Group are authentic and unchanged.

— — — — — — — —

Appendix F to Part 11

WORKED EXAMPLE: ACTIVE AUTHENTICATION (INFORMATIVE)

This worked example uses the following settings:

1.	Integer factorization-based mechanism:	RSA
2.	Modulus length (k):	1 024 bits (128 bytes)
3.	Hash algorithm:	SHA-1

Inspection system:

Step 1. Generate an 8 byte random:

RND.IFD = ‘F173589974BF40C6’

Step 2. Construct command for internal authenticate and send command APDU to the eMRTD’s contactless IC:

Command APDU

CLA	INS	P1	P2	Lc	Command data field	Le
00	88	00	00	08	RND.IFD	00

eMRTD’s contactless IC:

Step 3. Determine M_2 from incoming APDU:

M_2 = ‘F173589974BF40C6’

Step 4. Create the trailer:

T = ‘BC’ (i.e. SHA-1)

t (length of T in octets) = 1

Step 5. Determine lengths:

a. $c = k – L_h – 8t – 4 = 1024 – 160 – 8 – 4 = 852$ bits

b. $L_{M1} = c – 4 = 848$ bits

Step 6. Generate nonce M_1 of length L_{M1}:

M_1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’

Step 7. Create M:

M = M_1 | M_2 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6’

Step 8. Calculate SHA-1 digest of M:

H = SHA-1(M) = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

Step 9.[2] Construct the message representative:

F = ‘6A’ | M_1 | H | T =
‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC’

Step 10. Encrypt F with the Active Authentication Private Key to form the signature:

S = ‘756B683B036A6368F4A2EB29EA700F96
E26100AFC0809F60A91733BA29CAB362
8CB1A017190A85DADE83F0B977BB513F
C9C672E5C93EFEBBE250FE1B722C7CEE
F35D26FC8F19219C92D362758FA8CB0F
F68CEF320A8753913ED25F69F7CEE772
6923B2C43437800BBC9BC028C49806CF
2E47D16AE2B2CC1678F2A4456EF98FC9’

Step 11. Construct response data for INTERNAL AUTHENTICATE and send response APDU to the inspection system:

Response APDU:

Response data field	SW1-SW2
S	9000

2 Since the known part (RND.IFD) is not returned, but must be appended by the IFD itself, Partial Recovery applies (‘6A’).

Inspection system:

Step 12. Decrypt the signature with the public key:

F = ‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC’

Step 13. Determine hash algorithm by trailer T*:

T = ‘BC’ (i.e. SHA-1)

Step 14. Extract digest:

D = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

Step 15. Extract M_1:

M_1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’

Step 16. Header indicates partial recovery but signature has modulus length so concatenate M_1 with known M_2 (i.e. RND.IFD):

M* = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6’

Step 17. Calculate SHA-1 digest of M*:

D* = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

Step 18. Compare D and D*:

D is equal to D* so verification successful.

— — — — — — — —

Appendix G to Part 11

WORKED EXAMPLE: PACE – GENERIC MAPPING (INFORMATIVE)

This Appendix provides two worked examples for the PACE protocol as defined in Section 4.4 using the generic mapping. The first example is based on ECDH while the second one uses DH. All numbers contained in the tables are noted hexadecimal.

In both examples, the MRZ is used as password. This also leads to the same symmetric key K_{π}. The relevant data fields of the MRZ including the check digits are:

- Document Number: T220001293;
- Date of Birth: 6408125;
- Date of Expiry: 1010318.

Hence, the encoding K of the MRZ and the derived encryption key K_{π} are

K	7E2D2A41 C74EA0B3 8CD36F86 3939BFA8 E9032AAD
K_{π}	89DED1B2 6624EC1E 634C1989 302849DD

G.1 ECDH BASED EXAMPLE

This example is based on ECDH applying the standardized BrainpoolP256r1 domain parameters (see [RFC 5639]).

The first section introduces the corresponding `PACEInfo`. Subsequently, the exchanged APDUs including all generated nonces and ephemeral keys are listed and examined.

Elliptic Curve Parameters

Using standardized domain parameters, all information required to perform PACE is given by the data structure `PACEInfo`. In particular, no `PACEDomainParameterInfo` is needed.

PACEInfo	3012060A 04007F00 07020204 02020201 0202010D

The detailed structure of `PACEInfo` is itemized in the following table.

Tag	Length	Value	ASN.1 Type	Comment
30	12		SEQUENCE	PACEInfo
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	0D	INTEGER	Brainpool P256r1 Standardized Domain Parameters

For convenience, an ASN.1 encoding of the BrainpoolP256r1domain parameters is given below.

Tag	Length	Value	ASN.1 Type	Comment
30	81 EC		SEQUENCE	Domain parameter
06	07	2A 86 48 CE 3D 02 01	OBJECT IDENTIFIER	Algorithm id-ecPublicKey
30	81 E0		SEQUENCE	Domain Parameter
02	01	01	INTEGER	Version
30	2C		SEQUENCE	Underlying field
06	07	2A 86 48 CE 3D 01 01	OBJECT IDENTIFIER	Prime field
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 72 6E 3B F6 23 D5 26 20 28 20 13 48 1D 1F 6E 53 77	INTEGER	Prime p
30	44		SEQUENCE	Curve equation
04	20	7D 5A 09 75 FC 2C 30 57 EE F6 75 30 41 7A FF E7 FB 80 55 C1 26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9	OCTET STRING	Parameter a
04	20	26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9 BB D7 7C BF 95 84 16 29 5C F7 E1 CE 6B CC DC 18 FF 8C 07 B6	OCTET STRING	Parameter b

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
04	41		OCTET STRING	Group generator G
		04	-	Uncompressed point
		8B D2 AE B9 CB 7E 57 CB 2C 4B 48 2F FC 81 B7 AF B9 DE 27 E1 E3 BD 23 C2 3A 44 53 BD 9A CE 32 62	-	x-coordinate
		54 7E F8 35 C3 DA C4 FD 97 F8 46 1A 14 61 1D C9 C2 77 45 13 2D ED 8E 54 5C 1D 54 C7 2F 04 69 97	-	y-coordinate
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 71 8C 39 7A A3 B5 61 A6 F7 90 1E 0E 82 97 48 56 A7	INTEGER	Group order n
02	01	01	INTEGER	Cofactor f

Application flow of the ECDH-based example

To initialize PACE, the terminal sends the command MSE:Set AT to the chip.

T>C :	`00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 02 02 83 01 01`
C>T :	`90 00`

Here, T>C is an abbreviation for an APDU sent from terminal to chip while C>T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
Lc	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 02 02	Cryptographic mechanism: PACE with ECDH, generic mapping and AES128 session keys
	83	01	01	Password: MRZ

Response		
Status Bytes	90 00	Normal processing

Encrypted Nonce

Next, the chip randomly generates the nonce s and encrypts it by means of K_π.

Decrypted Nonce s	3F00C4D3 9D153F2B 2A214A07 8D899B22
Encrypted Nonce z	95A3A016 522EE98D 01E76CB6 B98B42C3

The encrypted nonce is queried by the terminal.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3 90 00

The encoding of the command APDU and the corresponding response can be found in the following table.

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	95 A3 A0 16 52 2E E9 8D 01 E7 6C B6 B9 8B 42 C3	Encrypted Nonce
Status Bytes	90 00		Normal processing	

Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

Terminal's Private Key	7F4EF07B 9EA82FD7 8AD689B3 8D0BC78C F21F249D 953BC46F 4C6E1925 9C010F99
Terminal's Public Key	7ACF3EFC 982EC455 65A4B155 129EFBC7 4650DCBF A6362D89 6FC70262 E0C2CC5E, 544552DC B6725218 799115B5 5C9BAA6D 9F6BC3A9 618E70C2 5AF71777 A9C4922D
Chip's Private Key	498FF497 56F2DC15 87840041 839A8598 2BE7761D 14715FB0 91EFA7BC E9058560
Chip's Public Key	824FBA91 C9CBE26B EF53A0EB E7342A3B F178CEA9 F45DE0B7 0AA60165 1FBA3F57, 30D8C879 AAA9C9F7 3991E61B 58F4D52E B87A0A0C 709A49DC 63719363 CCD13C54
Shared secret H	60332EF2 450B5D24 7EF6D386 8397D398 852ED6E8 CAF6FFEE F6BF85CA 57057FD5, 0840CA74 15BAF3E4 3BD414D3 5AA4608B 93A2CAF3 A4E3EA4E 82C9C13D 03EB7181
Mapped generator $\hat{G}$	8CED63C9 1426D4F0 EB1435E7 CB1D74A4 6723A0AF 21C89634 F65A9AE8 7A9265E2, 8C879506 743F8611 AC33645C 5B985C80 B5F09A0B 83407C1B 6A4D857A E76FE522

The following APDUs are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 45 7C 43 81 41 04 7A CF 3E FC 98 2E C4 55 65 A4 B1 55 12 9E FB C7 46 50 DC BF A6 36 2D 89 6F C7 02 62 E0 C2 CC 5E 54 45 52 DC B6 72 52 18 79 91 15 B5 5C 9B AA 6D 9F 6B C3 A9 61 8E 70 C2 5A F7 17 77 A9 C4 92 2D 00
C>T :	7C 43 82 41 04 82 4F BA 91 C9 CB E2 6B EF 53 A0 EB E7 34 2A 3B F1 78 CE A9 F4 5D E0 B7 0A A6 01 65 1F BA 3F 57 30 D8 C8 79 AA A9 C9 F7 39 91 E6 1B 58 F4 D5 2E B8 7A 0A 0C 70 9A 49 DC 63 71 93 63 CC D1 3C 54 90 00

The structure of the APDUs can be described as follows:

Command					
CLA	10		Command chaining		
INS	86		GENERAL AUTHENTICATE		
P1/P2	00 00		Keys and protocol implicitly known		
Lc	45		Length of data		
Data	Tag	Length	Value	Comment	
	7C	43	-	Dynamic Authentication Data	
	81	41		Mapping Data	
			04		Uncompressed Point
			7A CF 3E FC 98 2E ... C2 CC 5E		x-coordinate
			54 45 52 DC B6 72 ... C4 92 2D		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	82	41		Mapping Data	
			04		Uncompressed Point
			82 4F BA 91 C9 CB ... BA 3F 57		x-coordinate
			30 D8 C8 79 AA A9 ... D1 3C 54		y-coordinate
Status Bytes	90 00		Normal processing		

Perform Key Agreement

In the third step, chip and terminal perform an anonymous ECDH key agreement using the new domain parameters determined by the ephemeral group generator of the previous step. Only the x-coordinate is required as shared secret since the KDF uses only the first coordinate to derive the session keys.

Terminal's Private Key	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's Public Key	2DB7A64C 0355044E C9DF1905 14C625CB A2CEA487 54887122 F3A5EF0D 5EDD301C, 3556F3B3 B186DF10 B857B58F 6A7EB80F 20BA5DC7 BE1D43D9 BF850149 FBB36462
Chip's Private Key	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's Public Key	9E880F84 2905B8B3 181F7AF7 CAA9F0EF B743847F 44A306D2 D28C1D9E C65DF6DB, 7764B222 77A2EDDC 3C265A9F 018F9CB8 52E111B7 68B32690 4B59A019 3776F094
Shared Secret	28768D20 701247DA E81804C9 E780EDE5 82A9996D B4A31502 0B273319 7DB84925

The key agreement is performed as follows:

T>C :	10 86 00 00 45 7C 43 83 41 04 2D B7 A6 4C 03 55 04 4E C9 DF 19 05 14 C6 25 CB A2 CE A4 87 54 88 71 22 F3 A5 EF 0D 5E DD 30 1C 35 56 F3 B3 B1 86 DF 10 B8 57 B5 8F 6A 7E B8 0F 20 BA 5D C7 BE 1D 43 D9 BF 85 01 49 FB B3 64 62 00
C>T :	7C 43 84 41 04 9E 88 0F 84 29 05 B8 B3 18 1F 7A F7 CA A9 F0 EF B7 43 84 7F 44 A3 06 D2 D2 8C 1D 9E C6 5D F6 DB 77 64 B2 22 77 A2 ED DC 3C 26 5A 9F 01 8F 9C B8 52 E1 11 B7 68 B3 26 90 4B 59 A0 19 37 76 F0 94 90 00

The encoding of the key agreement is examined in the following table:

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	45		Length of data	
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	83	41		Terminal's Ephemeral Public Key
			04	Uncompressed Point

			2D B7 A6 4C 03 55 ... DD 30 1C		x-coordinate
			35 56 F3 B3 B1 86 ... B3 64 62		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	84	41		Chip's Ephemeral Public Key	
			04		Uncompressed Point
			9E 88 0F 84 29 05 ... 5D F6 DB		x-coordinate
			77 64 B2 22 77 A2 ... 76 F0 94		y-coordinate
Status Bytes	90 00		Normal processing		

By means of the KDF, the AES 128 session keys KS_{Enc} and KS_{MAC} are derived from the shared secret. These are

KS_{Enc}	F5F0E35C 0D7161EE 6724EE51 3A0D9A7F
KS_{MAC}	FE251C78 58B356B2 4514B3BD 5F4297D1

Mutual Authentication

The authentication tokens are derived by means of KS_{MAC} using

Input Data for T_{IFD}	7F494F06 0A04007F 00070202 04020286 41049E88 0F842905 B8B3181F 7AF7CAA9 F0EFB743 847F44A3 06D2D28C 1D9EC65D F6DB7764 B22277A2 EDDC3C26 5A9F018F 9CB852E1 11B768B3 26904B59 A0193776 F094
Input Data for T_{IC}	7F494F06 0A04007F 00070202 04020286 41042DB7 A64C0355 044EC9DF 190514C6 25CBA2CE A4875488 7122F3A5 EF0D5EDD 301C3556 F3B3B186 DF10B857 B58F6A7E B80F20BA 5DC7BE1D 43D9BF85 0149FBB3 6462

as input. The encoding of the input data is shown below

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	4F		PUBLIC KEY	Input data for T_{IFD}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's Ephemeral Public Point
		04		Uncompressed Point
		9E 88 0F 84 29 ... 5D F6 DB		x-coordinate
		77 64 B2 22 77 ... 76 F0 94		y-coordinate

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	4F		PUBLIC KEY	Input data for T_{IC}
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's Ephemeral Public Point
		04		Uncompressed Point
		2D B7 A6 4C 03 ... DD 30 1C		x-coordinate
		35 56 F3 B3 B1 ... B3 64 62		y-coordinate

The computed authentication tokens are:

T_{IFD}	C2B0BD78 D94BA866
T_{IC}	3ABB9674 BCE93C08

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 C2 B0 BD 78 D9 4B A8 66 00
C>T :	7C 0A 86 08 3A BB 96 74 BC E9 3C 08 90 00

G.2 DH BASED EXAMPLE

The second example is based on DH using the 1024-bit MODP Group with 160-bit Prime Order Subgroup specified by [RFC 5114]. The parameters of the group are:

Prime *p*	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup Generator *g*	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime Order *q* of *g*	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The first section introduces the `PACEInfo`. Subsequently, the exchanged APDUs including all generated nonces and ephemeral keys are listed and examined.

Diffie Hellman Parameters

The relevant information for PACE is given by the data structure `PACEInfo`.

PACEInfo	3012060A 04007F00 07020204 01020201 02020100

The detailed structure of `PACEInfo` is:

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
30	12		SEQUENCE	PACEInfo	
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER		OID: PACE with DH, generic mapping and AES 128 session keys
02	01	02	INTEGER		Version 2
02	01	00	INTEGER		Standardized 1024-bit Group specified by RFC 5114

Application flow of the DH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 01 02 83 01 01
C>T :	90 00

The encoding of the command is described in the next table.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
Lc	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 01 02	OID: Cryptographic mechanism: PACE with DH, generic mapping and AES128
	83	01	01	Password: MRZ
Response				
Status Bytes	90 00		Normal processing	

Encrypted Nonce

Next, the terminal queries a nonce from the chip.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	854D8DF5 827FA685 2D1A4FA7 01CDDDCA

The communication looks as follows.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA 90 00

The encoding of the command APDU and the corresponding response is described in the following table.

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	85 4D 8D F5 82 7F A6 85 2D 1A 4F A7 01 CD DD CA	Encrypted Nonce
Status Bytes	90 00		Normal processing	

Map Nonce

By means of the generic mapping, the nonce is mapped to an ephemeral group generator. For that purpose, the following ephemeral keys are randomly generated by terminal and chip.

Terminal's Private Key	5265030F 751F4AD1 8B08AC56 5FC7AC95 2E41618D
Terminal's Public Key	23FB3749 EA030D2A 25B278D2 A562047A DE3F01B7 4F17A154 02CB7352 CA7D2B3E B71C343D B13D1DEB CE9A3666 DBCFC920 B49174A6 02CB4796 5CAA73DC 702489A4 4D41DB91 4DE9613D C5E98C94 160551C0 DF86274B 9359BC04 90D01B03 AD54022D CB4F57FA D6322497 D7A1E28D 46710F46 1AFE710F BBBC5F8B A166F431 1975EC6C
Chip's Private Key	66DDAFEA C1609CB5 B963BB0C B3FF8B3E 047F336C
Chip's Public Key	78879F57 225AA808 0D52ED0F C890A4B2 5336F699 AA89A2D3 A189654A F70729E6 23EA5738 B26381E4 DA19E004 706FACE7 B235C2DB F2F38748 312F3C98 C2DD4882 A41947B3 24AA1259 AC22579D B93F7085 655AF308 89DBB845 D9E6783F E42C9F24 49400306 254C8AE8 EE9DD812 A804C0B6 6E8CAFC1 4F84D825 8950A91B 44126EE6
Shared secret H	5BABEBEF 5B74E5BA 94B5C063 FDA15F1F 1CDE9487 3EE0A5D3 A2FCAB49 F258D07F 544F13CB 66658C3A FEE9E727 389BE3F6 CBBBD321 28A8C21D D6EEA3CF 7091CDDF B08B8D00 7D40318D CCA4FFBF 51208790 FB4BD111 E5A968ED 6B6F08B2 6CA87C41 0B3CE0C3 10CE104E ABD16629 AA48620C 1279270C B0750C0D 37C57FFF E302AE7F
Mapped generator $\hat{G}$	7C9CBFE9 8F9FBDDA 8D143506 FA7D9306 F4CB17E3 C71707AF F5E1C1A1 23702496 84D64EE3 7AF44B8D BD9D45BF 6023919C BAA027AB 97ACC771 666C8E98 FF483301 BFA4872D EDE9034E DFACB708 14166B7F 36067682 9B826BEA 57291B5A D69FBC84 EF1E7790 32A30580 3F743417 93E86974 2D401325 B37EE856 5FFCDEE6 18342DC5

The following APDUs are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 86 7C 81 83 81 81 80 23 FB 37 49 EA 03 0D 2A 25 B2 78 D2 A5 62 04 7A DE 3F 01 B7 4F 17 A1 54 02 CB 73 52 CA 7D 2B 3E B7 1C 34 3D B1 3D 1D EB CE 9A 36 66 DB CF C9 20 B4 91 74 A6 02 CB 47 96 5C AA 73 DC 70 24 89 A4 4D 41 DB 91 4D E9 61 3D C5 E9 8C 94 16 05 51 C0 DF 86 27 4B 93 59 BC 04 90 D0 1B 03 AD 54 02 2D CB 4F 57 FA D6 32 24 97 D7 A1 E2 8D 46 71 0F 46 1A FE 71 0F BB BC 5F 8B A1 66 F4 31 19 75 EC 6C 00
C>T :	7C 81 83 82 81 80 78 87 9F 57 22 5A A8 08 0D 52 ED 0F C8 90 A4 B2 53 36 F6 99 AA 89 A2 D3 A1 89 65 4A F7 07 29 E6 23 EA 57 38 B2 63 81 E4 DA 1 9E0 04 70 6F AC E7 B2 35 C2 DB F2 F3 87 48 31 2F 3C 98 C2 DD 48 82 A4 19 47 B3 24 AA 12 59 AC 22 57 9D B9 3F 70 85 65 5A F3 08 89 DB B8 45 D9 E6 78 3F E4 2C 9F 24 49 40 03 06 25 4C 8A E8 EE 9D D8 12 A8 04 C0 B6 6E 8C AF C1 4F 84 D8 25 89 50 A9 1B 44 12 6E E6 90 00

The structure of the APDUs can be described as follows:

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	86		Length of data	
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	81	81 80	23 FB 37 49 EA 03 ... 75 EC 6C	Mapping Data
Le	00		Expected maximal byte length of the response data field is 256	

Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	82	81 80	ED 0F C8 90 A4 B2 ... 12 6E E6	Mapping Data
Status Bytes	90 00		Normal processing	

Perform Key Agreement

Subsequently, chip and terminal perform an anonymous DH key agreement using the new domain parameters determined by the ephemeral group generator of the previous step.

Terminal's Private Key	89CCD99B 0E8D3B1F 11E1296D CA68EC53 411CF2CA
Terminal's Public Key	00907D89 E2D425A1 78AA81AF 4A7774EC 8E388C11 5CAE6703 1E85EECE 520BD911 551B9AE4 D04369F2 9A02626C 86FBC674 7CC7BC35 2645B616 1A2A42D4 4EDA80A0 8FA8D61B 76D3A154 AD8A5A51 786B0BC0 71470578 71A92221 2C5F67F4 31731722 36B7747D 1671E6D6 92A3C7D4 0A0C3C5C E397545D 015C175E B5130551 EDBC2EE5 D4
Chip's Private Key	A5B78012 6B7C980E 9FCEA1D4 539DA1D2 7C342DFA
Chip's Public Key	075693D9 AE941877 573E634B 6E644F8E 60AF17A0 076B8B12 3D920107 4D36152B D8B3A213 F53820C4 2ADC79AB 5D0AEEC3 AEFB9139 4DA476BD 97B9B14D 0A65C1FC 71A0E019 CB08AF55 E1F72900 5FBA7E3F A5DC4189 9238A250 767A6D46 DB974064 386CD456 743585F8 E5D90CC8 B4004B1F 6D866C79 CE0584E4 9687FF61 BC29AEA1
Shared Secret	6BABC7B3 A72BCD7E A385E4C6 2DB2625B D8613B24 149E146A 629311C4 CA6698E3 8B834B6A 9E9CD718 4BA8834A FF5043D4 36950C4C 1E783236 7C10CB8C 314D40E5 990B0DF7 013E64B4 549E2270 923D06F0 8CFF6BD3 E977DDE6 ABE4C31D 55C0FA2E 465E553E 77BDF75E 3193D383 4FC26E8E B1EE2FA1 E4FC97C1 8C3F6CFF FE2607FD

The key agreement is performed as follows:

T>C :	10 86 00 00 86 7C 81 83 83 81 80 90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 74 EC 8E 38 8C 11 5C AE 67 03 1E 85 EE CE 52 0B D9 11 55 1B 9A E4 D0 43 69 F2 9A 02 62 6C 86 FB C6 74 7C C7 BC 35 26 45 B6 16 1A 2A 42 D4 4E DA 80 A0 8F A8 D6 1B 76 D3 A1 54 AD 8A 5A 51 78 6B 0B C0 71 47 05 78 71 A9 22 21 2C 5F 67 F4 31 73 17 22 36 B7 74 7D 16 71 E6 D6 92 A3 C7 D4 0A 0C 3C 5C E3 97 54 5D 01 5C 17 5E B5 13 05 51 ED BC 2E E5 D4 00
C>T :	7C 81 83 84 81 80 07 56 93 D9 AE 94 18 77 57 3E 63 4B 6E 64 4F 8E 60 AF 17 A0 07 6B 8B 12 3D 92 01 07 4D 36 15 2B D8 B3 A2 13 F5 38 20 C4 2A DC 79 AB 5D 0A EE C3 AE FB 91 39 4D A4 76 BD 97 B9 B1 4D 0A 65 C1 FC 71 A0 E0 19 CB 08 AF 55 E1 F7 29 00 5F BA 7E 3F A5 DC 41 89 92 38 A2 50 76 7A 6D 46 DB 97 40 64 38 6C D4 56 74 35 85 F8 E5 D9 0C C8 B4 00 4B 1F 6D 86 6C 79 CE 05 84 E4 96 87 FF 61 BC 29 AE A1 90 00

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	86		Length of data	
Data	Tag	Length	Value	Comment
	7C	81 83	-	Dynamic Authentication Data
	83	81 80	90 7D 89 E2 D4 25 ... 2E E5 D4	Terminal's Ephemeral Public Key
Le	00		Expected maximal byte length of the response data field is 256	

Response				
Data	Tag	Length	Value	Comment
	7C	81 83		Dynamic Authentication Data
	84	81 80	07 56 93 D9 AE 94 ... 29 AE A1	Chip's Ephemeral Public Key
Status Bytes	90 00		Normal processing	

The AES 128 session keys KS_{Enc} and KS_{MAC} are derived from the shared secret using the KDF.

KS_{Enc}	2F7F46AD CC9E7E52 1B45D192 FAFA9126
KS_{MAC}	805A1D27 D45A5116 F73C5446 9462B7D8

Mutual Authentication

The authentication tokens are constructed from the following input data.

Input Data for T_{IFD}	7F49818F 060A0400 7F000702 02040102 84818007 5693D9AE 94187757 3E634B6E 644F8E60 AF17A007 6B8B123D 9201074D 36152BD8 B3A213F5 3820C42A DC79AB5D 0AEEC3AE FB91394D A476BD97 B9B14D0A 65C1FC71 A0E019CB 08AF55E1 F729005F BA7E3FA5 DC418992 38A25076 7A6D46DB 97406438 6CD45674 3585F8E5 D90CC8B4 004B1F6D 866C79CE 0584E496 87FF61BC 29AEA1
Input Data for T_{IC}	7F49818F 060A0400 7F000702 02040102 84818090 7D89E2D4 25A178AA 81AF4A77 74EC8E38 8C115CAE 67031E85 EECE520B D911551B 9AE4D043 69F29A02 626C86FB C6747CC7 BC352645 B6161A2A 42D44EDA 80A08FA8 D61B76D3 A154AD8A 5A51786B 0BC07147 057871A9 22212C5F 67F43173 172236B7 747D1671 E6D692A3 C7D40A0C 3C5CE397 545D015C 175EB513 0551EDBC 2EE5D4

The encoding of the input data is shown below:

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
7F49	81 8F		PUBLIC KEY	Input data for T_{IFD}	
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER		PACE with DH, generic mapping and AES 128 session keys
84	81 80	07 56 93 D9 AE ... 29 AE A1	UNSIGNED INTEGER		Chip's Ephemeral Public Key

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
7F49	81 8F		PUBLIC KEY	Input data for T_{IC}	
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER		PACE with DH, generic mapping and AES 128 session keys
84	81 80	90 7D 89 E2 D4 ... 2E E5 D4	UNSIGNED INTEGER		Terminal's Ephemeral Public Key

The computed authentication tokens are:

T_{IFD}	B46DD9BD 4D98381F
T_{IC}	917F37B5 C0E6D8D1

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 B4 6D D9 BD 4D 98 38 1F 00
C>T :	7C 1B 86 08 91 7F 37 B5 C0 E6 D8 D1 87 0F 44 45 54 45 53 54 43 56 43 41 30 30 30 30 33

Command				
CLA	00		Plain	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	0C		Length of data	
Data	Tag	Length	Value	Comment
	7C	0A	-	Dynamic Authentication Data
	85	08	B4 6D D9 BD 4D 98 38 1F	Terminal's Authentication Token
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	0A		Dynamic Authentication Data
	86	08	91 7F 37 B5 C0 E6 D8 D1	Chip's Authentication Token
Status Bytes	90 00		Normal processing	

— — — — — — — —

Appendix H to Part 11

WORKED EXAMPLE: PACE – INTEGRATED MAPPING (INFORMATIVE)

This Appendix provides two examples for the PACE protocol with Integrated Mapping. The first one is based on Elliptic Curve Diffie-Hellman (ECDH) and the second one on Diffie-Hellman (DH). The MRZ-derived key *K* from the previous Example is used.

H.1 ECDH BASED EXAMPLE

This example is based on the BrainpoolP256r1 elliptic curve. The block cipher used in this example is AES-128. For reminder, the curve parameters are the following:

Prime p	A9FB57DB A1EEA9BC 3E660A90 9D838D72 6E3BF623 D5262028 2013481D 1F6E5377
Parameter a	7D5A0975 FC2C3057 EEF67530 417AFFE7 FB8055C1 26DC5C6C E94A4B44 F330B5D9
Parameter b	26DC5C6C E94A4B44 F330B5D9 BBD77CBF 95841629 5CF7E1CE 6BCCDC18 FF8C07B6
x-coordinate of the group generator G	8BD2AEB9 CB7E57CB 2C4B482F FC81B7AF B9DE27E1 E3BD23C2 3A4453BD 9ACE3262
y-coordinate of the group generator G	547EF835 C3DAC4FD 97F8461A 14611DC9 C2774513 2DED8E54 5C1D54C7 2F046997
Group order n	A9FB57DB A1EEA9BC 3E660A90 9D838D71 8C397AA3 B561A6F7 901E0E82 974856A7
Cofactor f	01

The encryption key is the following:

K_π	591468CD A83D6521 9CCCB856 0233600F

Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using $K_{\square}$. The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	2923BE84 E16CD6AE 529049F1 F1BBE9EB
Encrypted Nonce z	143DC40C 08C8E891 FBED7DED B92B64AD

Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p, derived from AES, is applied to s and t. Then, the point encoding f_G is used on the result to compute the Mapped Generator $\hat{G}=f_G(R_p(s,t))$.

Nonce t	5DD4CBFC 96F5453B 130D890A 1CDBAE32
Pseudo-random R(s,t)	E4447E2D FB3586BA C05DDB00 156B57FB B2179A39 49294C97 25418980 0C517BAA 8DA0FF39 7ED8C445 D3E421E4 FEB57322
$R_p(s,t)$	A2F8FF2D F50E52C6 599F386A DCB595D2 29F6A167 ADE2BE5F 2C3296AD D5B7430E
x-coordinate of the Mapped Generator $\hat{G}$	8E82D315 59ED0FDE 92A4D049 8ADD3C23 BABA94FB 77691E31 E90AEA77 FB17D427
y-coordinate of the Mapped Generator $\hat{G}$	4C1AE14B D0C3DBAC 0C871B7F 36081693 64437CA3 0AC243A0 89D3F266 C1E60FAD

Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator $\hat{G}$. The shared secret K is the x-coordinate of agreement.

Chip's private key SK_{IC}	107CF586 96EF6155 053340FD 633392BA 81909DF7 B9706F22 6F32086C 7AFF974A
Chip's public key PK_{IC}	67F78E5F 7F768608 2B293E8D 087E0569 16D0F74B C01A5F89 57D0DE45 691E51E8 932B69A9 62B52A09 85AD2C0A 271EE6A1 3A8ADDDC D1A3A994 B9DED257 F4D22753
Terminal's private key SK_{IFD}	A73FB703 AC1436A1 8E0CFA5A BB3F7BEC 7A070E7A 6788486B EE230C4A 22762595
Terminal's public key PK_{IFD}	89CBA23F FE96AA18 D824627C 3E934E54 A9FD0B87 A95D1471 DC1C0ABF DCD640D4 6755DE9B 7B778280 B6BEBD57 439ADFEB 0E21FD4E D6DF4257 8C13418A 59B34C37

Shared secret K	4F150FDE 1D4F0E38 E95017B8 91BAE171 33A0DF45 B0D3E18B 60BA7BEA FDC2C713

Using the specifications from [1], the session keys K_{Enc} and K_{MAC} are derived from K using the hash function SHA-1: K_{Enc}=SHA-1(K||0x00000001) and K_{MAC}=SHA-1(K||0x00000002). Then, only the first 16 octets of the digest are used with the following result:

K_{Enc}	0D3FEB33 251A6370 893D62AE 8DAAF51B
K_{MAC}	B01E89E3 D9E8719E 586B50B4 A7506E0B

Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC}.

Input data for T_{IC}	7F494F06 0A04007F 00070202 04040286 410489CB A23FFE96 AA18D824 627C3E93 4E54A9FD 0B87A95D 1471DC1C 0ABFDCD6 40D46755 DE9B7B77 8280B6BE BD57439A DFEB0E21 FD4ED6DF 42578C13 418A59B3 4C37
Input data for T_{IFD}	7F494F06 0A04007F 00070202 04040286 410467F7 8E5F7F76 86082B29 3E8D087E 056916D0 F74BC01A 5F8957D0 DE45691E 51E8932B 69A962B5 2A0985AD 2C0A271E E6A13A8A DDDCD1A3 A994B9DE D257F4D2 2753

The corresponding authentication tokens are:

T_{IC}	75D4D96E 8D5B0308
T_{IFD}	450F02B8 6F6A0909

H.2 DH BASED EXAMPLE

This example is based on the 1024-bit MODP Group with 160-bit Prime Order Subgroup. The block cipher used in this example is AES-128.

The group parameters are:

Prime p	B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371
Subgroup generator g	A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5
Prime order q of g	F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

The following encryption key is used:

K_π	591468CD A83D6521 9CCCB856 0233600F

Encrypted Nonce

A nonce s is randomly chosen by the chip and encrypted using K□. The encrypted nonce z is then sent to the terminal.

Decrypted Nonce s	FA5B7E3E 49753A0D B9178B7B 9BD898C8
Encrypted Nonce z	9ABB8864 CA0FF155 1E620D1E F4E13510

Map Nonce

A nonce t is randomly chosen and sent in clear. t and s are then used to compute the Integrated Mapping. First, the pseudo-random function R_p, derived from AES, is applied to s and t. Then, the point encoding f_g is used on the result.

Nonce t	B3A6DB3C 870C3E99 245E0D1C 06B747DE
Pseudo-random R(s,t)	EAB98D13 E0905295 2AA72990 7C3C9461 84DEA0FE 74AD2B3A F506F0A8 3018459C 38099CD1 F7FF4EA0 A078DB1F AC136550 5E3DC855 00EF95E2 0B4EEF2E 88489233 BEE0546B 472F994B 618D1687 02406791 DEEF3CB4 810932EC 278F3533 FDB860EB 4835C36F A4F1BF3F A0B828A7 18C96BDE 88FBA38A 3E6C35AA A1095925 1EB5FC71 0FC18725 8995944C 0F926E24 9373F485
$R_p(s,t)$	A0C7C50C 002061A5 1CC87D25 4EF38068 607417B6 EE1B3647 3CFB800D 2D2E5FA2 B6980F01 105D24FA B22ACD1B FA5C8A4C 093ECDFA FE6D7125 D42A843E 33860383 5CF19AFA FF75EFE2 1DC5F6AA 1F9AE46C 25087E73 68166FB0 8C1E4627 AFED7D93 570417B7 90FF7F74 7E57F432 B04E1236 819E0DFE F5B6E77C A4999925 328182D2
Mapped Generator $\hat{g}= f_g(R_p(s,t))$	1D7D767F 11E333BC D6DBAEF4 0E799E7A 926B9697 3550656F F3C83072 6D118D61 C276CDCC 61D475CF 03A98E0C 0E79CAEB A5BE2557 8BD4551D 0B109032 36F0B0F9 76852FA7 8EEA14EA 0ACA87D1 E91F688F E0DFF897 BBE35A47 2621D343 564B262F 34223AE8 FC59B664 BFEDFA2B FE7516CA 5510A6BB B633D517 EC25D4E0 BBAA16C2

Perform Key Agreement

The chip and the terminal perform an anonymous Diffie-Hellman key agreement using their secret keys and the mapped generator $\hat{g}$.

Chip's private key SK_{IC}	020F018C 7284B047 FA7721A3 37EFB7AC B1440BB3 0C5252BD 41C97C30 C994BB78 E9F0C5B3 2744D840 17D21FFA 6878396A 6469CA28 3EF5C000 DAF7D261 A39AB886 0ED4610A B5343390 897AAB5A 7787E4FA EFA0649C 6A94FDF8 2D991E8E 3FC332F5 142729E7 040A3F7D 5A4D3CD7 5CBEE1F0 43C1CAD2 DD484FEB 4ED22B59 7D36688E

Chip's public key PK_{IC}	928D9A0F 9DBA450F 13FC859C 6F290D1D 36E42431 138A4378 500BEB4E 0401854C FF111F71 CB6DC1D0 335807A1 1388CC8E AA87B079 07AAD9FB A6B169AF 6D8C26AF 8DDDC39A DC3AD2E3 FF882B84 D23E9768 E95A80E4 746FB07A 9767679F E92133B4 D379935C 771BD7FB ED6C7BB4 B1708B27 5EA75679 524CDC9C 6A91370C C662A2F3
Terminal's private key SK_{IFD}	4BD0E547 40F9A028 E6A515BF DAF96784 8C4F5F5F FF65AA09 15947FFD 1A0DF2FA 6981271B C905F355 1457B7E0 3AC3B806 6DE4AA40 6C1171FB 43DD939C 4BA16175 103BA3DE E16419AA 248118F9 0CC36A3D 6F4C3736 52E0C3CC E7F0F1D0 C5425B36 00F0F0D6 A67F004C 8BBA33F2 B4733C72 52445C1D FC4F1107 203F71D2 EFB28161
Terminal's public key PK_{IFD}	0F0CC629 45A80292 51FB7EF3 C094E12E C68E4EF0 7F27CB9D 9CD04C5C 4250FAE0 E4F8A951 557E929A EB48E5C6 DD47F2F5 CD7C351A 9BD2CD72 2C07EDE1 66770F08 FFCB3702 62CF308D D7B07F2E 0DA9CAAA 1492344C 85290691 9538C98A 4BA4187E 76CE9D87 832386D3 19CE2E04 3C3343AE AE6EDBA1 A9894DC5 094D22F7 FE1351D5
Shared secret K	419410D6 C0A17A4C 07C54872 CE1CBCEB 0A2705C1 A434C8A8 9A4CFE41 F1D78124 CA7EC52B DE7615E5 345E48AB 1ABB6E7D 1D59A57F 3174084D 3CA45703 97C1F622 28BDFDB2 DA191EA2 239E2C06 0DBE3BBC 23C2FCD0 AF12E0F9 E0B99FCF 91FF1959 011D5798 B2FCBC1F 14FCC24E 441F4C8F 9B08D977 E9498560 E63E7FFA B3134EA7

The session keys K_{Enc} and K_{MAC} are derived from K using the hash function SHA-1: K_{Enc}=SHA-1(K||0x00000001) and K_{MAC}=SHA-1(K||0x00000002). Then, only the first 16 octets of the digest are used with the following result:

K_{Enc}	01AFC10C F87BE36D 8179E873 70171F07
K_{MAC}	23F0FBD0 5FD6C7B8 B88F4C83 09669061

Mutual Authentication

The authentication tokens are computed using a CMAC on the following inputs with the key K_{MAC}.

Input data for T_{IC}	7F49818F 060A0400 7F000702 02040302 8481800F 0CC62945 A8029251 FB7EF3C0 94E12EC6 8E4EF07F 27CB9D9C D04C5C42 50FAE0E4 F8A95155 7E929AEB 48E5C6DD 47F2F5CD 7C351A9B D2CD722C 07EDE166 770F08FF CB370262 CF308DD7 B07F2E0D A9CAAA14 92344C85 29069195 38C98A4B A4187E76 CE9D8783 2386D319 CE2E043C 3343AEAE 6EDBA1A9 894DC509 4D22F7FE 1351D5
Input data for T_{IFD}	7F49818F 060A0400 7F000702 02040302 84818092 8D9A0F9D BA450F13 FC859C6F 290D1D36 E4243113 8A437850 0BEB4E04 01854CFF 111F71CB 6DC1D033 5807A113 88CC8EAA 87B07907 AAD9FBA6 B169AF6D 8C26AF8D DDC39ADC 3AD2E3FF 882B84D2 3E9768E9 5A80E474 6FB07A97 67679FE9 2133B4D3 79935C77 1BD7FBED 6C7BB4B1 708B275E A7567952 4CDC9C6A 91370CC6 62A2F3

The corresponding authentication tokens are:

T_{IC}	C2F04230 187E1525
T_{IFD}	55D61977 CBF5307E

— — — — — — — —

Appendix I to Part 11

WORKED EXAMPLE: PACE – PACE CA MAPPING (INFORMATIVE)

This Appendix provides an example for the PACE protocol with Chip Authentication Mapping based on Elliptic Curve Diffie-Hellman (ECDH). All numbers contained in the tables are noted hexadecimal.

The MRZ is used as password. The relevant data fields of the MRZ including the check digits are:

- Document Number: C11T002JM4;
- Date of Birth: 9608122;
- Date of Expiry: 2310314.

Hence, the encoding K of the MRZ and the derived encryption key K_π are

K	894D03F1 48C6265E 89845B21 8856EA34 D00EF8E8
K_π	4E6F6FBF 7BE748B9 32C7B741 61BBA9DF

I.1 ECDH BASED EXAMPLE

This example is based on ECDH applying the standardized BrainpoolP256r1 domain parameters (see [RFC 5639]).

The first section introduces the corresponding `PACEInfo`. Subsequently, the exchanged APDUs including all generated nonces and ephemeral keys are listed and examined.

Elliptic Curve Parameters

Using standardized domain parameters, all information required to perform PACE is given by the data structure `PACEInfo`. In particular, no `PACEDomainParameterInfo` is needed.

PACEInfo	3012060A 04007F00 07020204 06020201 0202010D

The detailed structure of `PACEInfo` is itemized in the following table.

Tag	Length	Value	ASN.1 Type	Comment
30	12		SEQUENCE	PACEInfo
06	0A	04 00 7F 00 07 02 02 04 06 02	OBJECT IDENTIFIER	PACE with ECDH, Chip Authentication Mapping and AES 128 session keys
02	01	02	INTEGER	Version 2
02	01	0D	INTEGER	Brainpool P256r1 Standardized Domain Parameters

For convenience, an ASN.1 encoding of the BrainpoolP256r1domain parameters is given below.

Tag	Length	Value	ASN.1 Type	Comment
30	81 EC		SEQUENCE	Domain parameter
06	07	2A 86 48 CE 3D 02 01	OBJECT IDENTIFIER	Algorithm id-ecPublicKey
30	81 E0		SEQUENCE	Domain Parameter
02	01	01	INTEGER	Version
30	2C		SEQUENCE	Underlying field
06	07	2A 86 48 CE 3D 01 01	OBJECT IDENTIFIER	Prime field
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 72 6E 3B F6 23 D5 26 20 28 20 13 48 1D 1F 6E 53 77	INTEGER	Prime p
30	44		SEQUENCE	Curve equation
04	20	7D 5A 09 75 FC 2C 30 57 EE F6 75 30 41 7A FF E7 FB 80 55 C1 26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9	OCTET STRING	Parameter a
04	20	26 DC 5C 6C E9 4A 4B 44 F3 30 B5 D9 BB D7 7C BF 95 84 16 29 5C F7 E1 CE 6B CC DC 18 FF 8C 07 B6	OCTET STRING	Parameter b

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
04	41		OCTET STRING	Group generator G
		04	-	Uncompressed point
		8B D2 AE B9 CB 7E 57 CB 2C 4B 48 2F FC 81 B7 AF B9 DE 27 E1 E3 BD 23 C2 3A 44 53 BD 9A CE 32 62	-	x-coordinate
		54 7E F8 35 C3 DA C4 FD 97 F8 46 1A 14 61 1D C9 C2 77 45 13 2D ED 8E 54 5C 1D 54 C7 2F 04 69 97	-	y-coordinate
02	21	00 A9 FB 57 DB A1 EE A9 BC 3E 66 0A 90 9D 83 8D 71 8C 39 7A A3 B5 61 A6 F7 90 1E 0E 82 97 48 56 A7	INTEGER	Group order n
02	01	01	INTEGER	Cofactor f

Application flow of the ECDH-based example

To initialize PACE, the terminal sends the command MSE:AT to the chip.

T>C :	`00 22 C1 A4 0F 80 0A 04 00 7F 00 07 02 02 04 06 02 83 01 01`
C>T :	`90 00`

Here, T>C is an abbreviation for an APDU sent from terminal to chip while C>T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

Command				
CLA	00		Plain	
INS	22		Manage security environment	
P1/P2	C1 A4		Set Authentication Template for mutual authentication	
Lc	0F		Length of data field	
Data	Tag	Length	Value	Comment
	80	0A	04 00 7F 00 07 02 02 04 06 02	Cryptographic mechanism: PACE with ECDH, Chip Authentication Mapping and AES128 session keys
	83	01	01	Password: MRZ

Response		
Status Bytes	90 00	Normal processing

Encrypted Nonce

Next, the chip randomly generates the nonce s and encrypts it by means of K_π.

Decrypted Nonce s	658B860B C94DF6F0 44FCE6D5 C82CF8E5
Encrypted Nonce z	CB60E8E0 D85B76A9 BD304747 C2AD42E2

The encrypted nonce is queried by the terminal.

T>C :	10 86 00 00 02 7C 00 00
C>T :	7C 12 80 10 CB 60 E8 E0 D8 5B 76 A9 BD 30 47 47 C2 AD 42 E2 90 00

The encoding of the command APDU and the corresponding response can be found in the following table.

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	02		Length of data	
Data	Tag	Length	Value	Comment
	7C	00	-	Absent
Le	00		Expected maximal byte length of the response data field is 256	
Response				
Data	Tag	Length	Value	Comment
	7C	12		Dynamic Authentication Data
	80	10	CB60E8E0 D85B76A9 BD304747 C2AD42E2	Encrypted Nonce
Status Bytes	90 00		Normal processing	

Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

Terminal's Private Key	5D8BB87B D74D985A 4B7D4325 B9F7B976 FE835122 77340079 8914AA22 738135CC
Terminal's Public Key	7F1D410A DB7DDB3B 84BF1030 800981A9 105D7457 B4A3ADE0 02384F30 86C67EDE 1AB88910 4A27DB6D 842B0190 20FBF3CE ACB0DC62 7F7BDCAC 29969E19 D0E553C1
Chip's Private Key	9E56A6B5 9C95D06E CE5CD10F 983BB2F4 F1943528 E577F238 81D89D8C 3BBEE0AA
Chip's Public Key	A234236A A9B9621E 8EFB73B5 245C0E09 D2576E52 77183C12 08BDD552 80CAE8B3 04F36571 3A356E65 A451E165 ECC9AC0A C46E3771 342C8FE5 AEDD0926 85338E23
Shared secret H	2C1DCC17 73346492 C6636A36 EE4B965E 292E9AAE 7EE37736 EF58B9D0 A043F348 403A8CF3 3CA7DC0D 9DF61D08 89CE2442 4FF97C1A AD48A5CA 2A554B07 1EF7638D
Mapped generator $\hat{G}$	89F0B5EA BF3BE293 C75903A3 98613192 5C9F5B51 5CA95AF4 85DC7E88 6F03245D 44BEFB2D D3A0DBD7 1CB5E618 971CF474 7F12B79E 548379A4 0E45963B AAF3E829

The following APDUs are exchanged by terminal and chip to map the nonce.

T>C :	10 86 00 00 45 7C 43 81 41 04 7F 1D 41 0A DB 7D DB 3B 84 BF 10 30 80 09 81 A9 10 5D 74 57 B4 A3 AD E0 02 38 4F 30 86 C6 7E DE 1A B8 89 10 4A 27 DB 6D 84 2B 01 90 20 FB F3 CE AC B0 DC 62 7F 7B DC AC 29 96 9E 19 D0 E5 53 C1 00
C>T :	7C 43 82 41 04 A2 34 23 6A A9 B9 62 1E 8E FB 73 B5 24 5C 0E 09 D2 57 6E 52 77 18 3C 12 08 BD D5 52 80 CA E8 B3 04 F3 65 71 3A 35 6E 65 A4 51 E1 65 EC C9 AC 0A C4 6E 37 71 34 2C 8F E5 AE DD 09 26 85 33 8E 23 90 00

The structure of the APDUs can be described as follows:

Command					
CLA	10		Command chaining		
INS	86		GENERAL AUTHENTICATE		
P1/P2	00 00		Keys and protocol implicitly known		
Lc	45		Length of data		
Data	Tag	Length	Value	Comment	
	7C	43	-	Dynamic Authentication Data	
	81	41		Mapping Data	
			04		Uncompressed Point
			7F 1D 41 0A ... 86 C6 7E DE		x-coordinate
			1A B8 89 10... D0 E5 53 C1		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	82	41		Mapping Data	
			04		Uncompressed Point
			A2 34 23 6A ... 80 CA E8 B3		x-coordinate
			04 F3 65 71... 85 33 8E 23		y-coordinate
Status Bytes	90 00		Normal processing		

Perform Key Agreement

In the third step, chip and terminal perform an anonymous ECDH key agreement using the new domain parameters determined by the ephemeral group generator of the previous step. Only the x-coordinate is required as shared secret since the KDF uses only the first coordinate to derive the session keys.

Terminal's Private Key	76ECFDAA 9841C323 A3F5FC5E 88B88DB3 EFF7E35E BF57A7E6 946CB630 006C2120
Terminal's Public Key	446C9340 84D9DAB8 63944F21 9520076C 29EE3F7A E6722B11 FF319EC1 C7728F95 5483400B FF60BF0C 59292700 09277DC2 A515E125 75010AD9 BA916CF1 BF86FEFC
Chip's Private Key	CD626EF3 C256E235 FE8912CA C28279E6 26008EDA 6B3A05C4 CF862A3B DAB79E78
Chip's Public Key	02AD566F 3C6EC7F9 324509AD 50A51FA5 2030782A 4968FCFE DF737DAE A9933331 11C3B9B4 C2287789 BD137E7F 8AA882E2 A3C633CC D6ECC2C6 3C57AD40 1A09C2E1
Shared Secret	67950559 D0C06B4D 4B86972D 14460837 461087F8 419FDBC3 6AAF6CEA AC462832

The key agreement is performed as follows:

T>C :	10 86 00 00 45 7C 43 83 41 04 44 6C 93 40 84 D9 DA B8 63 94 4F 21 95 20 07 6C 29 EE 3F 7A E6 72 2B 11 FF 31 9E C1 C7 72 8F 95 54 83 40 0B FF 60 BF 0C 59 29 27 00 09 27 7D C2 A5 15 E1 25 75 01 0A D9 BA 91 6C F1 BF 86 FE FC 00
C>T :	7C 43 84 41 04 02 AD 56 6F 3C 6E C7 F9 32 45 09 AD 50 A5 1F A5 20 30 78 2A 49 68 FC FE DF 73 7D AE A9 93 33 31 11 C3 B9 B4 C2 28 77 89 BD 13 7E 7F 8A A8 82 E2 A3 C6 33 CC D6 EC C2 C6 3C 57 AD 40 1A 09 C2 E1 90 00

The encoding of the key agreement is examined in the following table:

Command				
CLA	10		Command chaining	
INS	86		GENERAL AUTHENTICATE	
P1/P2	00 00		Keys and protocol implicitly known	
Lc	45		Length of data	
Data	Tag	Length	Value	Comment
	7C	43	-	Dynamic Authentication Data
	83	41		Terminal's Ephemeral Public Key
			04	Uncompressed Point

			44 6C 93 40 ... C7 72 8F 95		x-coordinate
			54 83 40 0B ... BF 86 FE FC		y-coordinate
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	43		Dynamic Authentication Data	
	84	41		Chip's Ephemeral Public Key	
			04		Uncompressed Point
			02 AD 56 6F ... A9 93 33 31		x-coordinate
			11 C3 B9 B4 ... 1A 09 C2 E1		y-coordinate
Status Bytes	90 00		Normal processing		

By means of the KDF, the AES 128 session keys KS_{Enc} and KS_{MAC} are derived from the shared secret. These are

KS_{Enc}	0A9DA4DB 03BDDE39 FC5202BC 44B2E89E
KS_{MAC}	4B1C0649 1ED5140C A2B537D3 44C6C0B1

Mutual Authentication

The authentication tokens are derived by means of KS_{MAC} using

Input Data for T_{IFD}	7F494F06 0A04007F 00070202 04060286 410402AD 566F3C6E C7F93245 09AD50A5 1FA52030 782A4968 FCFEDF73 7DAEA993 333111C3 B9B4C228 7789BD13 7E7F8AA8 82E2A3C6 33CCD6EC C2C63C57 AD401A09 C2E1
Input Data for T_{IC}	7F494F06 0A04007F 00070202 04060286 4104446C 934084D9 DAB86394 4F219520 076C29EE 3F7AE672 2B11FF31 9EC1C772 8F955483 400BFF60 BF0C5929 27000927 7DC2A515 E1257501 0AD9BA91 6CF1BF86 FEFC

as input. The encoding of the input data is shown below.

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	4F		PUBLIC KEY	Input data for T_{IFD}
06	0A	04 00 7F 00 07 02 02 04 06 02	OBJECT IDENTIFIER	PACE with ECDH, Chip Authentication Mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's Ephemeral Public Point
		04		Uncompressed Point
		02 AD 56 6F... A9 93 33 31		x-coordinate
		11 C3 B9 B4 ... 1A 09 C2 E1		y-coordinate

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***
7F49	4F		PUBLIC KEY	Input data for T_{IC}
06	0A	04 00 7F 00 07 02 02 04 06 02	OBJECT IDENTIFIER	PACE with ECDH, Chip Authentication Mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's Ephemeral Public Point
		04		Uncompressed Point
		44 6C 93 40 ... C7 72 8F 95		x-coordinate
		54 83 40 0B ... BF 86 FE FC		y-coordinate

The computed authentication tokens are:

T_{IFD}	E86BD060 18A1CD3B
T_{IC}	8596CF05 5C67C1A3

Finally, these tokens are exchanged and verified.

T>C :	00 86 00 00 0C 7C 0A 85 08 E8 6B D0 60 18 A1 CD 3B 00
C>T :	7C 3C 86 08 85 96 CF 05 5C 67 C1 A3 8A 30 1E EA 96 4D AA E3 72 AC 99 0E 3E FD E6 33 33 53 BF C8 9A 67 04 D9 3D A8 79 8C F7 7F 5B 7A 54 BD 10 CB A3 72 B4 2B E0 B9 B5 F2 8A A8 DE 2F 4F 92 90 00

The encoding of the mutual authentication is examined in the following table:

Command					
CLA	00		No command chaining (last command in chain)		
INS	86		GENERAL AUTHENTICATE		
P1/P2	00 00		Keys and protocol implicitly known		
Lc	0C		Length of data		
Data	Tag	Length	Value	Comment	
	7C	0A	-	Dynamic Authentication Data	
	85	08		Terminal's Authentication Token	
			E8 6B D0 60 18 A1 CD 3B		T_{IFD}
Le	00		Expected maximal byte length of the response data field is 256		
Response					
Data	Tag	Length	Value	Comment	
	7C	3C		Dynamic Authentication Data	
	86	08		Chip's Authentication Token	
			85 96 CF 05 5C 67 C1 A3		T_{IC}
	8A	30			x-coordinate
			1E EA 96 4D … DE 2F 4F 92		Encrypted Chip Authentication Data
Status Bytes	90 00		Normal processing		

Chip Authentication

Get `ChipAuthenticationPublicKeyInfo` from EF.CardSecurity

ChipAuthenticationPublicKeyInfo	`30620609 04007F00 07020201 02305230`
	`0C060704 007F0007 01020201 0D034200`
	`04187270 9494399E 7470A643 1BE25E83`
	`EEE24FEA 568C2ED2 8DB48E05 DB3A610D`
	`C884D256 A40E35EF CB59BF67 53D3A489`
	`D28C7A4D 973C2DA1 38A6E7A4 A08F68E1`
	`6F02010D`

The detailed structure of `ChipAuthenticationPublicKeyInfo` is itemized in the following table.

Tag	***Length***	***Value***	***ASN.1 Type***	***Comment***	
30	62		SEQUENCE	ChipAuthenticationPublicKeyInfo	
06	09	04 00 7F 00 07 02 02 01 02	OBJECT IDENTIFIER		id-PK-ECDH
30	52		SEQUENCE		SubjectPublicKeyInfo
30	0C		SEQUENCE		Brainpool P256r1 Standardized Domain Parameters
06	07	04 00 7F 00 07 01 02	OBJECT IDENTIFIER		standardizedDomainParameters
02	01	0D	INTEGER		Brainpool256r1
03	42	00 04 18 72 70 … 8F 68 E1 6F	BIT STRING		CA Public Key
02	01	0D	INTEGER		keyID 13

For Chip Authentication the following data is used:

Encrypted Chip Authentication Data	1EEA964D AAE372AC 990E3EFD E6333353 BFC89A67 04D93DA8 798CF77F 5B7A54BD 10CBA372 B42BE0B9 B5F28AA8 DE2F4F92
Decrypted Chip Authentication Data	85DC3FA9 3D0952BF A82F5FD1 89EE75BD 82F11D1F 0B8ED4BF 5319AC9B 53C426B3
IV for De-/Encryption of CA Data IV = $E(KS_{ENC}, -1)$	F6A3B75A1 E933941 DD7A13E2 520779DF
Chip's Public Key from GENERAL AUTHENTICATE Mapping Nonce $PK_{MAP,IC}$	A234236A A9B9621E 8EFB73B5 245C0E09 D2576E52 77183C12 08BDD552 80CAE8B3 04F36571 3A356E65 A451E165 ECC9AC0A C46E3771 342C8FE5 AEDD0926 85338E23
Chip's Public CA Key from ChipAuthenticationPublicKeyInfo PK_{IC}	18727094 94399E74 70A6431B E25E83EE E24FEA56 8C2ED28D B48E05DB 3A610DC8 84D256A4 0E35EFCB 59BF6753 D3A489D2 8C7A4D97 3C2DA138 A6E7A4A0 8F68E16F

Terminal verifies that $PK_{MAP,IC} = KA(CA_{IC}, PK_{IC}, D_{IC})$.

Appendix J to Part 11

INSPECTION PROCEDURES (INFORMATIVE)

J.1 Inspection Procedure for eMRTD Application

This section describes an inspection procedure which contains only an eMRTD Application (“LDS1-documents”).

1. Gain access to the contactless IC (see section 4.2)

    - If access to the IC is protected, PACE or BAC can be used in this step, although it is recommended to use PACE for security reasons. Beginning 1/1/2018 eMRTDs may support PACE only.

    - If supported by IC and terminal, PACE-CAM should be used for performance reasons.

    - The IC grants access to less sensitive data in the eMRTD Application and to EF.CardSecurity in the Master File, if present.

2. Start authentication of data

    - Read the Document Security Object and verify the signature, including chain verification of the Document Signer Certificate.

3. Authentication of the chip

    - Depending on support by the IC, perform Chip Authentication or Active Authentication. Support of Active Authentication is indicated by the presence of EF.DG15 in the eMRTD Application, support for Chip Authentication by the presence of corresponding `SecurityInfo`s in EF.DG14.

    - This step can also be performed as part of step 1, if PACE with Chip Authentication Mapping is used.

    - Authentication is only complete in combination with authentication of the file containing the public key (EF.CardSecurity, EF.DG14 or EF.DG15) used for this step.

4. Additional access control

    - Performing Terminal Authentication is necessary, if the eMRTD is configured to require this for access to sensitive data, i.e. EF.DG3 and/or EF.DG4.

5. Read data

    - Reading data can be started as soon as the necessary access rights are granted, e.g. less sensitive data can be read after step 1.

    - Data must not be considered genuine without authentication of the read data (step 2).

J.2 Inspection Procedure for multi-application eMRTDs

This section describes an inspection procedure designed for eMRTDs containing one or more applications besides the eMRTD Application ("LDS2-documents"). This procedure can also be used to access the eMRTD Application only.

1. Gain access to the contactless IC (see section 4.2)

    - In this setting, only PACE is available to gain access to the IC.
    - If supported by IC and terminal, PACE-CAM should be used for performance reasons.
    - The IC grants access to less sensitive data in the eMRTD Application and to EF.CardSecurity in the Master File.

2. Check presence of EF.CardSecurity

    - If EF.CardSecurity is not present, the eMRTD does not support authentication in the Master File (implying that the IC only contains an eMRTD Application). In this case select the eMRTD Application and continue with step 2 of the procedure in Appendix J.1.

3. Start authentication of data

    - Read EF.CardSecurity and verify the signature, including chain verification of the Document Signer Certificate.
    - Data from the eMRTD Application are protected via the Document Security Object, which must be verified when data from this application is read. Data from other applications are protected by signatures of the data, which also must be verified upon reading these data.

4. Authentication of the chip

    - Perform Chip Authentication in the Master File. If the necessary information are not contained in the `SecurityInfos` in EF.CardSecurity, the IC does not support authentication in the Master File. In this case select the eMRTD Application and continue with step 2 of the procedure in Appendix J.1.
    - This step can also be performed as part of step 1, if PACE with Chip Authentication Mapping is used.
    - Authentication is only complete in combination with authentication of the file containing the public key (EF.CardSecurity) used for this step.

5. Additional access control

    - Perform Terminal Authentication.
    - If only read access to less sensitive data in the eMRTD Application is required, this step can be skipped.

6. Reading/writing data

    - Reading/writing data includes selection of the applications containing the files.
    - Reading data can be started as soon as the necessary access rights are granted, e.g. less sensitive data of the eMRTD Application can be read after step 1.

- Data must not be considered genuine without authentication of the read data (step 3).

Appendix K to Part 11

EUROPEAN EXTENDED ACCESS CONTROL (INFORMATIVE)

Terminal Authentication as defined in this document is based on Extended Access Control as used in the European Union (see [TR-03110]) to protect access to fingerprints stored in the LDS1-application. This Appendix points out the differences between [TR-03110] and the protocols defined in this document.

The Advanced Inspection Procedure used to access eMRTDs equipped with EAC according to [TR-03110] comprises the following steps:

1. Perform the Chip Access Procedure (see section 4.2) and select the eMRTD Application;

2. Perform Chip Authentication in the eMRTD Application (see section 6.2) and start Passive Authentication (see section 5.1);

3. Perform Terminal Authentication (see below) in the eMRTD Application (see section 7.1).

Note.— Both Chip and Terminal Authentication are performed in the eMRTD Application in the European Extended Access Control. The specifications in this document allow these protocols – depending on context – to be performed either in the eMRTD Application or the Master File.

K.1 Access Rights

Table K.1: Authorization of Inspection Systems

7 6	5 4 3 2 1 0	Description
x x	- - - - - -	Role (see Doc 9303-12)
- -	x x x x x x	Access Rights
- -	x x x x - -	RFU
- -	- - - - 1 -	Read access to eMRTD Application: DG 4 (Iris)
- -	- - - - - 1	Read access to eMRTD Application: DG 3 (Fingerprint)

Access rights to data groups in applications other than the eMRTD Application are conveyed via Authorization Extensions as defined in Parts 12 and 10 of Doc 9303. Access rights for fingerprints (and iris) are conveyed via the Certificate Holder Authorization Template:

For the computation of the effective access rights see section 7.1.4.3.6.

K.2 EF.CVCA

According to the specification, the trust points (Certificate Authority References) known to the IC for certificate verification as part of Terminal Authentication are transmitted to the IFD as part of the PACE protocol (see section 4.4.3.5).

The European Extended Access Control defines a transparent file EF.CVCA in the eMRTD Application instead. The specification is reproduced below:

Table K.2: Elementary File EF.CVCA

File Name	EF.CVCA
File ID	0x011C (default)
Short File ID	0x1C (default)
Read Access	PACE
Write Access	NEVER (internally updated only)
Size	36 bytes (fixed) padded with octets of value 0x00
Content	$[CAR_i][\|\|CAR_{i-1}][\|\|0x00..00]$

If the IC supports Terminal Authentication in the eMRTD Application, it MUST make the references of CVCA public keys suitable for inspection systems available in a transparent elementary file EF.CVCA in the eMRTD Application as specified in Table K.2.

This file SHALL contain a sequence of Certification Authority Reference (CAR) data objects (see Doc 9303-12) suitable for Terminal Authentication.

- It SHALL contain at most two Certification Authority Reference data objects.
- The most recent Certification Authority Reference SHALL be the first data object in this list.
- The file MUST be padded by appending octets of value 0x00.

The file EF.CVCA has a default EF identifier and short EF identifier. If the default values cannot be used, the (short) EF identifier SHALL be specified in the OPTIONAL parameter `efCVCA` of the `TerminalAuthenticationInfo`. If `efCVCA` is used to indicate the EF identifier to be used, the default EF identifier is overridden. If no short EF identifier is given in `efCVCA`, the file EF.CVCA MUST be explicitly selected using the given EF identifier.

```
TerminalAuthenticationInfo ::= SEQUENCE {
  protocol OBJECT IDENTIFIER(id-TA),
  version  INTEGER, -- MUST be 1
  efCVCA   FileID OPTIONAL
}

FileID ::= SEQUENCE {
  fid  OCTET STRING (SIZE(2)),
  sfid OCTET STRING (SIZE(1)) OPTIONAL
}
```

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2020

Part 12: Public Key Infrastructure for MRTDs

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 12 — *Public Key Infrastructure for MRTDs*
ISBN 978-92-9249-800-9

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

1. SCOPE

Part 12 defines the Public Key Infrastructure (PKI) for the eMRTD application. Requirements for issuing States or organizations are specified, including operation of a Certification Authority (CA) that issues certificates and Certificate Revocation Lists (CRLs). Requirements for receiving States and their Inspection Systems validating those certificates and CRLs are also specified.

The Eight Edition of Doc 9303 incorporates the specifications for Visible Digital Seals (known as VDS) and for the optional Travel Records, Visa Records and Additional Biometric Applications (known as LDS2) as an extension of the mandatory eMRTD application (known as LDS1).

Doc 9303-12 shall be read in conjunction with:

- Doc 9303-10 — *Logical Data Structure (LDS) for Storage of Biometrics and other data in the Contactless Integrated Circuit (IC)*; and
- Doc 9303-11 — *Security Mechanisms for MRTDs*.
- Doc 9303-13 – Visible Digital Seals

2. OVERVIEW OF THE PUBLIC KEY INFRASTRUCTURE

The eMRTD Public Key Infrastructure (PKI) enables the creation and subsequent verification of digital signatures on eMRTD objects, including the Document Security Object (SO_D) to ensure the signed data is authentic and has not been modified. Revocation of a certificate, failure of the certification path validation procedure or failure of digital signature verification does not on its own cause an eMRTD to be considered invalid. Such a failure means that the electronic verification of the integrity and authenticity of the LDS data has failed and other non-electronic mechanisms could then be used to make that determination as part of the overall inspection of the eMRTD.

The eMRTD PKI is much simpler than more generic multi-application PKIs such as the Internet PKI defined in [RFC 5280]. In the eMRTD PKI, each issuing State/Authority establishes a single Certification Authority (CA) that issues all certificates directly to end-entities, including Document Signers. These CAs are referred to as Country Signing Certification Authorities (CSCAs). There are no other CAs in the infrastructure. Receiving States establish trust directly in the keys/certificates of each issuing State or organization's CSCA.

The eMRTD PKI is based on generic PKI standards including [X.509] and [RFC 5280]. Those base PKI standards define a large set of optional features and complex trust relationships among CAs that are not relevant to the eMRTD application. A profile of those standards, tailored to the eMRTD application, is specified in this Part of Doc 9303. Some of the unique aspects of the eMRTD application include:

- there is precisely one CSCA per issuing State;
- certification paths include precisely one certificate (e.g. Document Signer);
- signature verification must be possible 5-10 years after creation;
- CSCA name change is supported; and
- CSCA Link certificates are not processed as intermediate certificates in a certification path.

For the most part, the eMRTD PKI infrastructure is compliant with [RFC 5280]. However, the fact that CSCAs can undergo a name change imposes unique requirements on the eMRTD PKI that are incompatible with some of the CRL validation procedures defined in [RFC 5280]. These differences have been kept to a minimum and are clearly identified.

For VDS and LDS2, the Digital Signature PKI, which provides integrity and authenticity of the data objects, is an extension of the LDS1 PKI. The Signers for VDS and LDS2 are issued by the same CSCA which issues Signers for LDS1. The changes to the Certificate Profiles for these new applications are specified in this document. Taken together, this infrastructure is referred to as the **eMRTD PKI**.

The Digital Signature PKI consists of the following entities:

- Country Signing CA (CSCA)
- Document Signer Certificates (DSC) which is used to sign the SOD
- LDS2 Signer Certificates, which consists of the following:
    - LDS2-TS Signer – signs LDS2 Travel Stamps
    - LDS2-V Signer – signs LDS2 Electronic Visas
    - LDS2-B Signer – signs LDS2 Additional Biometrics
- Bar Code Signer Certificates (BCSC), for which the following two specific types are defined in this document:
    - Visa Signer Certificates (VSC)
    - Emergency Travel Document Signer Certificates (ESC)
- Master List Signer Certificates (MSC) used to sign Master Lists
- Deviation List Signer Certificates (DLSC) used to sign Deviation Lists
- Certificate Revocation List (CRL)

All the different certificate types are signed by the same CSCA. The CSCA also signs the CRL, which contains any revoked certificate irrespective of the type of certificate. All the certificates issued under the CSCA are collectively referred to as **Signer Certificates**.

For LDS2 applications, a separate **Authorization PKI** is defined. The authorization PKI enables the eMRTD Issuing State or organization to control and manage the foreign States that are given authorization to write LDS2 data objects to their eMRTDs and to read those data objects. A foreign State intending to read or write LDS2 data must obtain an authorization certificate directly from the eMRTD Issuing State or organization.

The Authorization PKI uses a different certificate structure (ISO 7816 card verifiable certificates) and therefore requires additional infrastructure components.

LDS2 requires the terminal to prove to the eMRTD contactless IC that it is entitled to write LDS2 data objects to the contactless IC or that it is entitled to read LDS2 data objects. Such a terminal is equipped with at least one private key and the corresponding Terminal Certificate, encoding the terminal's public key and access rights. After the terminal has proven knowledge of this private key, the MRTD chip grants the terminal access to read/write LDS2 data as indicated in the Terminal Certificate.

The LDS2 authorization PKI consists of the following entities:

- Country Verifying CAs (CVCAs)
- Document Verifiers (DVs)
- Terminals
- Single Point of Contact (SPOC)

Distribution and management of the authorization certificates between CVCAs in one State and DVs in other States is handled through a Single Point of Contact (SPOC) in each State.

This Part 12 of Doc 9303 specifies the eMRTD PKI profile, the Authorization PKI profile and corresponding objects including:

- roles and responsibilities of entities in the infrastructure;
- cryptographic algorithms and key management;
- certificate and CRL content;
- certificate and CRL distribution mechanisms; and
- certification path validation.

3. ROLES AND RESPONSILITIES

This section details the entities and the roles and responsibilities of both the eMRTD PKI and the Authorization PKI.

3.1 eMRTD PKI

The authenticity and integrity of data stored on eMRTDs is protected by Passive Authentication. This security mechanism is based on digital signatures and consists of the following PKI entities for eMRTD PKI:

- **Country Signing CA (CSCA):** Each issuing State/Authority establishes a single CSCA as its national trust point in the context of eMRTDs. The CSCA issues public key certificates for one or more (national) Document Signers and optionally for other end-entities such as Master List Signers and Deviation List Signers. The CSCA also issues periodic Certificate Revocation Lists (CRL) indicating whether any of the issued certificates have been revoked.

- **Document Signers (DS):** A Document Signer digitally signs data to be stored on eMRTDs; this signature is stored on the eMRTD in a Document Security Object.

- **LDS2 Signers**: An LDS2 Signer digitally signs LDS2 data objects of one or more types.

- **Bar Code Signer (BCS):** A Bar Code Signer digitally signs the data (header and message) encoded in the bar code. The signature is also stored in the bar code. This document specifies two use cases for the use of Bar Code Signer, viz. Visa and Emergency Travel Documents.

- **Inspection Systems (IS):** An Inspection System verifies the digital signature, including certification path validation to verify the authenticity and integrity of the electronic data stored on the eMRTD as part of Passive Authentication.

- **Master List Signers:** A Master List Signer is an optional entity that digitally signs a list of CSCA certificates (domestic and foreign) in support of the bilateral distribution mechanism for CSCA certificates.

- **Deviation List Signers** is used to sign Deviation Lists. Deviation lists are defined in Doc 9303-3.

The secure facilities to generate key pairs SHALL be under the control of the issuing State or organization. Each key pair includes a “private” key and a “public” key. The private keys and associated systems or facilities SHALL be well protected from any outside or unauthorized access through inherent design and hardware security facilities.

While the CSCA certificate remains relatively static, a large number of Document Signer certificates will be created over time.

The CSCA of each issuing State or organization acts as the trust point for the receiving State. The issuing State or organization distributes its own CSCA public key to receiving States in the form of a certificate. The receiving State establishes that this certificate (and certified key) are “trusted” through out-of-band means, and stores a “Trust Anchor” for that trusted key/certificate. These CSCA certificates SHALL be self-signed certificates issued directly by the CSCA. CSCA certificates MUST NOT be subordinate or cross certificates in a larger PKI infrastructure. CSCA self-issued link certificates may also be issued to help the receiving State in establishing trust in a new CSCA key/certificate following a key-rollover.

Note.— In some States there is a requirement that a centralized Controller of Certification Authority (CCA) be the supreme authority to publish self-signed certificates for all applications. In these cases, a possible solution is for the CSCA to create a self-signed certificate (satisfying the ICAO Doc 9303 requirements) and have that certificate countersigned by the CCA (satisfying the State’s own CCA requirement). However, these countersigned certificates are not part of the eMRTD PKI and would not be distributed to receiving States.

3.1.1 Country Signing Certification Authority

It is RECOMMENDED that CSCA key pairs (KPu_{CSCA}, KPr_{CSCA}) be generated and stored in a highly protected, off-line CA infrastructure.

The CSCA private key (KPr_{CSCA}) is used to sign Document Signer certificates (C_{DS}), other certificates and CRLs.

Country Signing Certification Authority certificates (C_{CSCA}) are used to validate Document Signer certificates, Master List Signer certificates, Deviation List Signer certificates, CRLs and other certificates issued by the CSCA.

All certificates and CRLs MUST comply with the profiles specified in Section 7 and MUST be distributed using the distribution mechanisms as specified in Section 5.

For PKD participants, each CSCA certificate (C_{CSCA}) MUST also be forwarded by the certificate issuer to the PKD (for the purpose of validation of Document Signer certificates (C_{DS})).

CRLs MUST be issued on a periodic basis as specified in Section 4.

3.1.2 Document Signers

It is RECOMMENDED that Document Signer key pairs (KPu_{DS}, KPr_{DS}) be generated and stored in a highly protected infrastructure.

The Document Signer private key (KPr_{DS}) is used to sign Document Security Objects (SO_D).

Document Signer certificates (C_{DS}) are used to validate Document Security Objects (SO_D).

Each Document Signer certificate (C_{DS}) MUST comply with the certificate profile defined in Section 7 and MUST be stored in the contactless IC of each eMRTD that was signed with the corresponding DS private key (see Doc 9303-10 for details). This ensures that the receiving State has access to the Document Signer certificate relevant to each eMRTD.

Document Signer certificates of PKD participants SHOULD also be forwarded by the certificate issuer to ICAO for publication in the ICAO Public Key Directory (PKD).

3.1.3 LDS2 Signers

An LDS2 Signer digitally signs LDS2 data objects of one or more types.

Where there is a need to refer to an LDS2 Signer as one that signs a particular LDS2 data object type, it is referred to as follows:

- LDS2-TS Signer – signs LDS2 Travel Stamps
- LDS2-V Signer – signs LDS2 Electronic Visas
- LDS2-B Signer – signs LDS2 Additional Biometrics

It is RECOMMENDED that each State have no more than one LDS2-TS Signer, one LDS2-V Signer and one LDS2-B Signer. It is also possible for one LDS2 Signer to combine some/all of these roles.

If further differentiation is required, such as the location a travel stamp was added, the individual officer who cleared a traveler, which officer granted a visa, or the location at which additional biometrics were added, these details can be included in a proprietary field within the respective LDS2 data object itself.

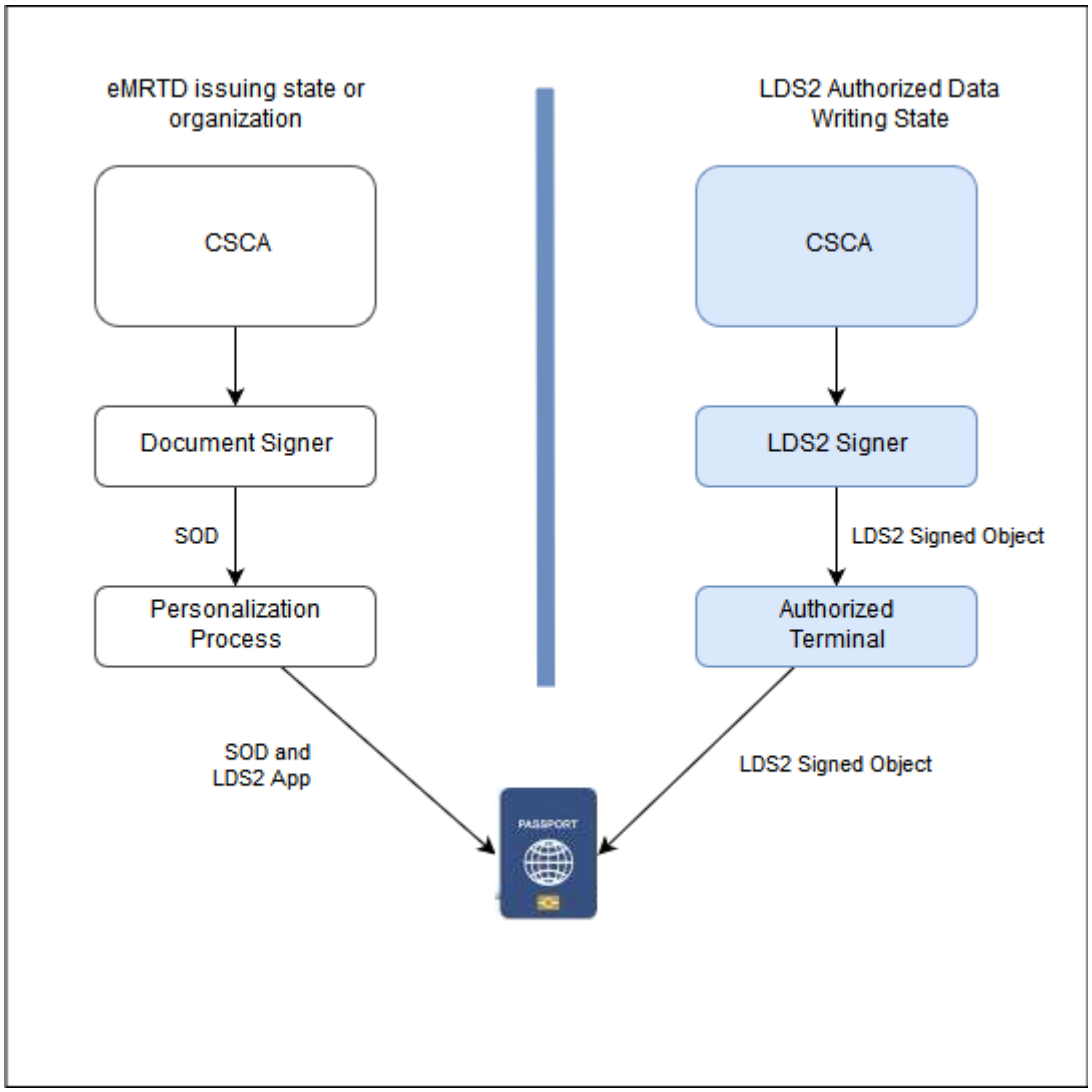


Figure 1 : LDS2 Trust Model and Writing Architecture

3.1.4 Bar Code Signers

It is RECOMMENDED that Bar Code Signer key pairs (KPu_{BCS}, KPr_{BCS}) be generated and stored in a highly protected infrastructure.

The Bar Code Signer private key (KPr_{BCS}) is used to sign the data (header and message) encoded in the bar code. The signature is also stored in the bar code.

Bar Code Signer certificates (C_{BCS}) are used to validate the data (header and message) encoded in the bar code.

Each Bar Code Signer certificate (C_{BCS}) MUST comply with the certificate profile defined in Section 7. The bar code Signer Certificates are not contained in the digital seal itself. Hence, a country that issues documents protected with digital seals MUST publish all its bar code Signer Certificates. The primary distribution channel for bar code Signer Certificates is PKD/bilateral. Other mechanisms, e.g. publication on a website, are secondary channels.

Bar Code Signer certificates of PKD participants SHOULD also be forwarded by the certificate issuer to ICAO for publication in the ICAO Public Key Directory (PKD).

The Visa Signer (VS) and Emergency Travel Document Signer are special case of the Bar Code Signer.

3.1.5 Inspection System

Inspection Systems perform Passive Authentication to ensure the integrity and authenticity of the data stored on the eMRTD contactless IC. As part of that process, Inspection Systems MUST perform certification path validation as indicated in Section 6.

3.1.6 Master List Signer

The Master List Signer private key is used to sign CSCA Master Lists.

Master List Signer certificates are used to validate CSCA Master Lists.

3.1.7 Deviation List Signer

The Deviation List Signer private key is used to sign Deviation Lists.

Deviation List Signer certificates are used to validate Deviation Lists.

3.2 Authorization PKI

The LDS2 application is written to the contactless IC of an eMRTD, by the Issuing State or organization at the time of personalization.

Before another State can write LDS2 objects to that contactless IC, it MUST obtain authorization from the Issuing State or organization to do so. Each LDS2 data object is digitally signed by an LDS2 Signer in the writing State and subsequently written to the contactless IC by an authorized terminal in that writing State. The two step process of signing by a signer and writing by an authorized terminal is similar to the LDS1 concept where the Document Signer digitally signs Document Security Objects but they are subsequently written to the contactless IC through the personalization process, as illustrated in Figure 1. Subsequent reading of LDS2 objects from the contactless IC is done through terminals authorized for LDS2 reading of the LDS2 object type in question.

The authorization PKI enables the eMRTD Issuing State or organization to control access (read and write) to LDS2 data on contactless ICs in eMRTDs it issues.

3.2.1 Country Verifying Certificate Authority

Each issuing State or organization that allows LDS2 data to be added to its eMRTDs MUST set up a single CVCA. This CVCA is a Certification Authority (CA) that is the trust anchor for the authorization PKI of that State or organization and covers all the LDS2 applications. The CVCA may be a stand-alone entity or it may be integrated with the CSCA of that same State or organization. However, even if co-located, the CVCA MUST use a different key pair than that of the CSCA. The CVCA determines the access rights that will be granted to all Document Verifiers (DV), foreign and domestic and issues certificates containing the individual authorizations to each of those DVs.

3.2.2 Document Verifier

A Document Verifier is a CA that, as part of an organizational unit, manages a group of terminals (e.g. terminals operated by a State's border police) and issues authorization certificates to those terminals. A DV MUST have already received an authorization certificate from the responsible CVCA before it can issue associated certificates to its terminals. Certificates issued by a DV to terminals MAY contain the same authorization, or a subset, that has been granted to the DV. They MUST NOT contain any authorization beyond that granted to the DV.

3.2.3 Terminal/Inspection System

Within the context of the authorization PKI, a terminal is the entity that accesses the contactless IC of an eMRTD and writes a digitally signed LDS2 data object, or reads an LDS2 data object. The terminal MUST have an authorization certificate issued to it, from its local DV that grants the required authorization. The terminal is also referred to as an Inspection System.

3.2.4 Single Point of Contact (SPOC)

Each State that participates in the LDS2 authorization PKI MUST set up a single SPOC. This SPOC is the interface that is used for all communication between the CVCA of one State with the DVs in another State. Certificate requests and responses are communicated between the SPOCs of each State using the SPOC protocol defined in Section 8.

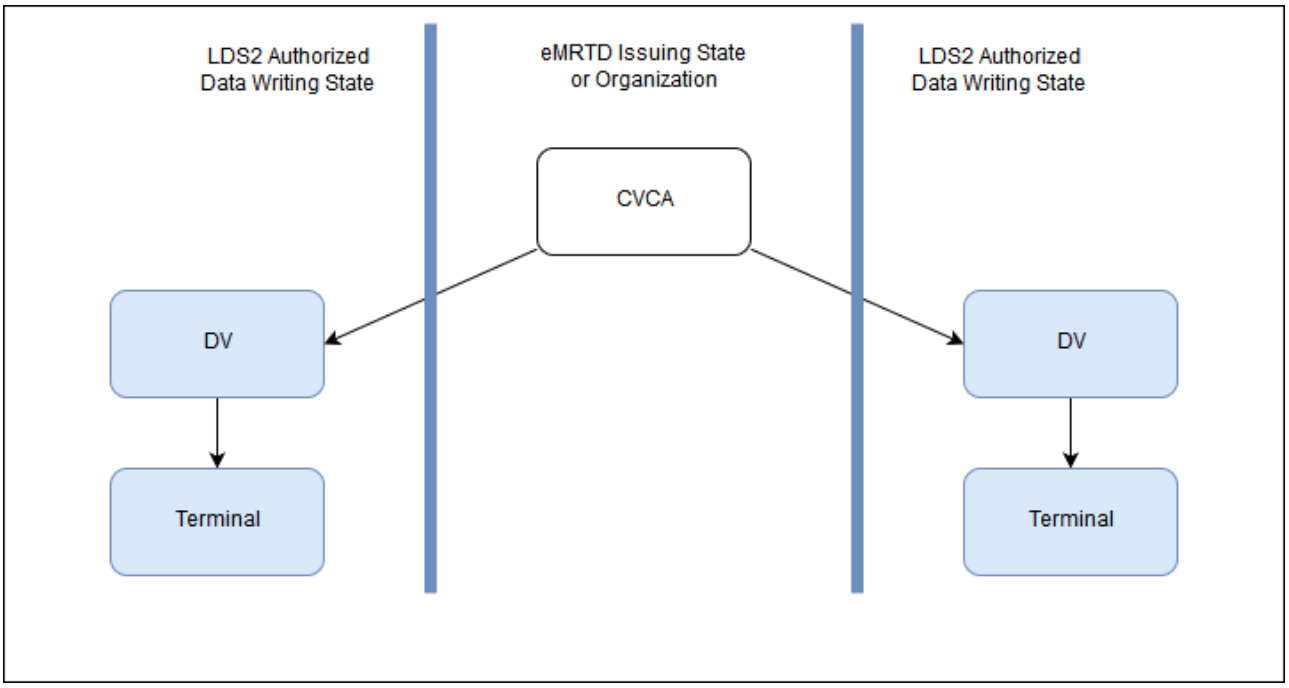


Figure 2 : Authorization PKI Trust Model

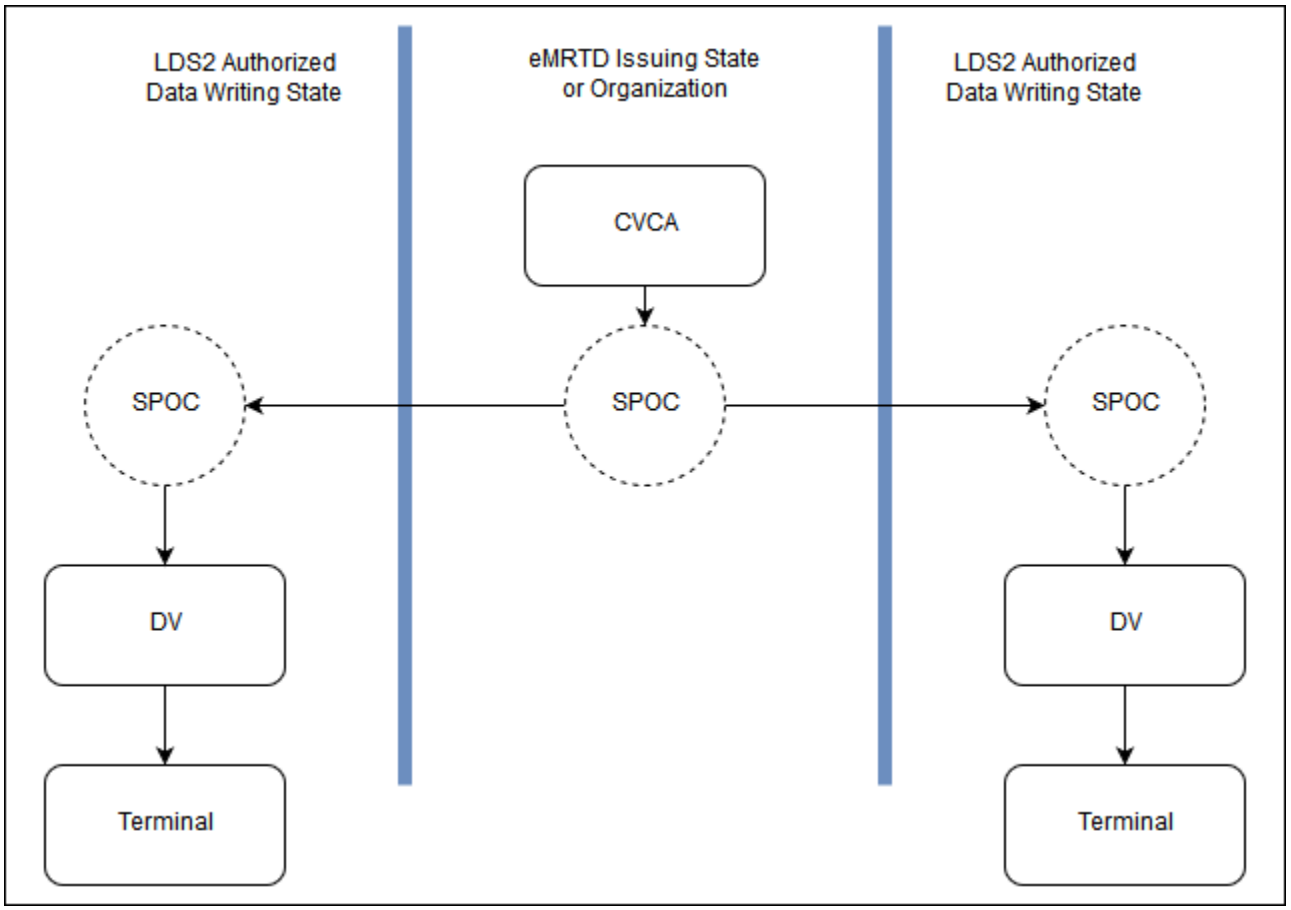


Figure 3 : SPOC Role

4. KEY MANAGEMENT

Key Management is defined for the two Public Key Infrastructures separately.

4.1 eMRTD PKI

Issuing States or organizations SHALL have at least two key pair types:

- Country Signing CA key pair; and
- Document Signer key pair.

Issuing States or organizations MAY have additional key pair types:

- Master List Signer key pair;
- Deviation List Signer key pair.
- LDS2 Signer key pair
- SPOC client key pair
- SPOC server key pair
- Visa Signer key pair/Emergency Travel Document Signer key pair (both are type of Bar Code Signer).

The Country Signing CA, Signer Certificate and SPOC certificate public keys are issued using [X.509] certificates. The public keys contained in CSCA certificates are used to verify the CSCA signature on issued Signer Certificates, SPOC Certificates, CSCA and on issued CRLs.

For Master List Signer, Deviation List Signer and Communications keys and certificates, the private key lifetime and the certificate validity period are left to the discretion of the issuing State or organization.

Both the CSCA certificates and Document Signer certificates are associated with a private key usage and a public key validity period as outlined in Table 1.

Table 1. Key Usage and Validity

	Use of Private Key	***Public Key Validity (assuming 10-year valid passports)***
Country Signing CA	3-5 years	13-15 years
Document Signer	Up to 3 months[1]	approx. 10 years
LDS2-TS Signer	1-2 years	10 years + 3 months
LDS2-V Signer	1-2 years	10 years + 3 months
LDS2-B Signer	1-2 years	10 years + 3 months
SPOC Client	Not Specified	6-18 months

1 Note the corresponding `privateKeyUsage` extension in DS certificate might be slightly longer to allow for overlap or production requirements.

	Use of Private Key	***Public Key Validity (assuming 10-year valid passports)***
SPOC Server	Not Specified	6-18 months
Visa Bar Code Signer	1-2 years	Private Key Usage Time + Validity of Visa
Emergency Travel Document Bar Code Signer	1 year + 2 months (the 2 month are meant for smooth roll-over)	Private Key Usage Time + ETD validity timeframe
Master List Signer	Discretion of issuing State or organization	Discretion of issuing State or organization
Deviation List Signer	Discretion of issuing State or organization	Discretion of issuing State or organization
Communication	Discretion of issuing State or organization	Discretion of issuing State or organization

4.1.1 Document Signer Keys and Certificates

The usage period of a Document Signer private key is much shorter than the validity period of the DS certificate for the corresponding public key.

4.1.1.1 Document Signer Public Key validity

The lifetime, i.e. the certificate validity period, of the Document Signer public key is determined by concatenating the following two periods:

- the length of time the corresponding private key will be used to issue eMRTDs, with;
- the longest validity period of any eMRTD issued under that key[2].

The Document Signer certificate (C_{DS}) SHALL be valid for this total period to enable the authenticity of eMRTDs to be verified. However the corresponding private key SHOULD only be used to issue documents for a limited period; once the last document it was used to issue has expired, the public key is no longer required.

4.1.1.2 Document Signer Private Key issuing period

When deploying their systems, issuing States or organizations may wish to take into account the number of documents that will be signed by any one individual Document Signer private key.

An issuing State or organization may deploy one or more Document Signers, each with its own unique key pair, that are active at any given time.

In order to minimize business continuity costs in the event of a Document Signer certificate being revoked, an issuing State or organization that issues a large number of eMRTDs per day may wish to:

- use a very short private key usage period; and/or
- deploy several concurrent Document Signers that are active at the same time, each with its own unique private key and public key certificate.

2 Some issuing States or organizations may issue eMRTDs before they become valid, for instance on a change of name upon marriage. In these situations, the “longest validity period of any eMRTD” includes the actual validity of the eMRTD (e.g. 10 years) plus the maximum time between when the eMRTD is issued and the time it becomes valid.

An issuing State or organization that issues a small number of eMRTDs per day may choose to deploy a single Document Signer and may also be comfortable with a slightly longer private key usage period.

Regardless of the number of eMRTDs issued per day, or number of Document Signers active at the same time, it is RECOMMENDED that the maximum period any Document Signer private key is used to sign eMRTDs be three months.

Once the last document signed with a given private key has been produced, it is RECOMMENDED that issuing States or organizations erase the private key in an auditable and accountable manner.

4.1.2 LDS2 Signer Keys and Certificates

LDS2 Signer key pairs are similar to Document Signer key pairs in that the usage period of the private key is much shorter than the validity period of the corresponding certificate. The certificates MUST remain valid for the lifetime of the eMRTD or the signed LDS2 object (whichever is longest). Because signed data objects will be written to eMRTDs from various States, these certificates MUST be valid for at least the duration of the longest eMRTD lifetime (i.e. 10 years).

4.1.2.1 LDS2 Signer Public Key Validity

The lifetime, i.e. the certificate validity period, of the LDS2 Signer public key is determined by concatenating the following two periods:

- The length of time the corresponding private key will be used to sign LDS2 objects, with;
- The validity period of whichever of the following is longest:
  - Any eMRTD that will store an LDS2 object signed with that key; or
  - Any LDS2 object signed with that key. Note that in the case of LDS2 eVisa, it is possible for the validity period of a signed eVisa to extend beyond the validity period of the eMRTD including that visa.

4.1.3 Bar Code Signer Keys and Certificates

A bar code Signer is a specific type of signature server used to sign a unique Document Type Category, e.g. a visa, Emergency Travel Document etc. To follow the best practices in the field, it is RECOMMENDED that only a limited number of signing keys (a lower one-digit number) is used in parallel to create signatures for digital seals, unless operational requirements make a larger number of keys absolutely necessary. To ensure availability of the bar code Signer in case of a security incident related to the signing keys, it is RECOMMENDED to have measures in place to ensure business continuity (e.g. preparation of backup keys, backup site, etc.).

In order to facilitate the handling of the corresponding certificates (see Section 5), the number of published signature validation keys MUST be limited to five signature keys per year.

4.1.3.1 Bar Code Signer Public Key Validity

This section applies to all Bar Code Signers, including Visa Signer and Emergency Travel Document Signer.

The lifetime, i.e. the certificate validity period, of the Bar Code Signer public key is determined by concatenating the following two periods:

- the length of time the corresponding private key will be used to issue a Visa or ETD, with;
- the longest validity period of any document issued under that key[3].

The Bar Code Signer certificate SHALL be valid for this total period to enable the authenticity of document to be verified. However the corresponding private key SHOULD only be used to issue documents for a limited period; once the last document it was used to issue has expired, the public key is no longer required.

3 Some issuing States or organizations may issue eMRTDs before they become valid, for instance on a change of name upon marriage. In these situations, the “longest validity period of any eMRTD” includes the actual validity of the eMRTD (e.g. 10 years) plus the maximum time between when the eMRTD is issued and the time it becomes valid.

Private Key Usage Time:	As per document profile
Certificate Validity:	Private Key Usage Time + document Validity Timeframe

Example

Note: The actual validity periods used for the calculation this example do not imply any recommendations.

Suppose documents with a validity period of 5 years are issued, and the private key usage time of the bar code Signer Certificate is 1 year. Then validity of the bar code Signer Certificate is 1 + 5 = 6 years. If the usage time of the private key of the CSCA Certificate is 3 years, then the validity of the CSCA Certificate is 3 + 6 = 9 years.

4.1.4 CSCA Keys and Certificates

The usage period of a CSCA private key is much shorter than the validity period of the CSCA certificate for the corresponding public key.

4.1.4.1 Country Signing CA Public Key validity

The lifetime, i.e. the certificate validity, of the CSCA public key is determined by concatenating the following periods:

- the length of time the corresponding CSCA private key will be used to sign any certificate below the CSCA; and,
- the maximum key lifetime of any certificate issued below the CSCA.

4.1.4.2 Country Signing CA Private Key issuing period

The usage period for the CSCA private key to sign certificates and CRLs is a delicate balance among the following factors:

- In the unlikely event of an issuing State or organization Country Signing Private CA Key being compromised, then the validity of all eMRTDs issued using Document Signer Keys whose certificates were signed by the compromised CSCA private key is called into doubt. Consequently issuing States or organizations MAY wish to keep the issuing period quite short;
- Keeping the issuing period very short, however, leads to having a very large number of CSCA public keys valid at any one time. This can lead to more complex certificate management within the border processing systems.

It is therefore RECOMMENDED that an issuing State or organization's CSCA key pair be replaced every three to five years.

4.1.4.3 Country Signing CA Re-key

CSCA keys provide the trust points in the whole system and without these the system would collapse. Therefore issuing States or organizations SHOULD plan the replacement of their CSCA key pair carefully. Once the issuance period for the initial CSCA private signing key has elapsed, an issuing State or organization will always have at least two CSCA certificates (C_{CSCA}) valid at any one time.

Issuing States or organizations MUST notify receiving States that a CSCA key rollover is planned. This notification MUST be provided 90 days in advance of the key rollover. Once the key rollover has occurred the new CSCA certificate (certifying the new CSCA public key) is distributed to receiving States.

If the CSCA certificate is a new self-signed certificate, authentication of that certificate should be done using an out-of-band method.

When a CSCA key rollover occurs a certificate MUST be issued that links the new key to the old key to provide a secure transition for relying parties. Generally this is achieved through the issuance of a self-issued-certificate where the issuer and subject fields are identical but the key used to verify the signature represents the old key pair and the certified public key

represents the new key pair. These CSCA Link certificates need not be verified using an out-of-band method as the signature on the CSCA Link certificate is verified using an already trusted public key for that CSCA. Master Lists can also be used to distribute CSCA Link and CSCA self-signed root certificates.

Issuing States or organizations should refrain from using their new CSCA private key for the first two days after the CSCA key rollover, to ensure the corresponding new CSCA public key certificate has been distributed successfully.

Issuing States or organizations MUST use the newest CSCA private key for signing all certificates, and for signing CRLs.

4.1.5 Certificate Revocation

Issuing States or organizations may need to revoke certificates in case of an incident (like a key compromise).

All CSCAs MUST produce periodic revocation information in the form of a Certificate Revocation List (CRL).

CSCAs MUST issue at least one CRL every 90 days, even if no certificates have been revoked since the previous CRL was issued. CRLs MAY be issued more frequently than every 90 days but not more frequently than every 48 hours.

If a certificate is revoked, a CRL indicating that revocation MUST be distributed within 48 hours.

Only certificates can be revoked, not Document Security Objects. The use of CRLs is limited to notifications of revoked certificates that had been issued by the CSCA that issued the CRL (including revocation notices for CSCA certificates, DS certificates, Master List Signer certificates, Deviation List Signer certificates and any other certificate types issued by that CA).

Partitioned CRLs are not used in the eMRTD application. All certificates revoked by a CSCA, including DS certificates, CSCA certificates, Master List Signer certificates and Deviation List Signer certificates are listed on the same CRL. Although the CRL is always signed with the newest (current) CSCA private signing key, the CRL includes revocation notices for certificates signed with that same private key as well as certificates signed with earlier CSCA private signing keys.

4.1.5.1 Revocation of CSCA Certificates

Revocation of a CSCA certificate is both extreme and difficult. Upon informing a receiving State that a CSCA certificate has been revoked, all other certificates signed using the corresponding CSCA private key are effectively revoked.

Where a CSCA Link certificate has been signed using an old CSCA private key to certify a new CSCA public key (see “Country Signing Re-key” in 4.2), revoking the old CSCA certificate SHALL also revoke the new CSCA certificate.

If a CSCA certificate needs to be revoked, the CSCA may issue a CRL signed with the private key that corresponds to the public key being revoked, as this is the only key users of the CRL will be able to verify at that time. The CSCA public key should be considered valid only for the purpose of verifying that CRL signature. Once a CRL user has verified the CRL signature, the CSCA private signing key is considered compromised and the certificate revoked for all future verifications.

To issue new documents, the issuing State or organization MUST revert to bootstrapping its authentication process from the beginning, by issuing a new CSCA Root certificate, distributing that certificate to receiving States, and supporting out-of-band confirmation that the certificate received by each receiving State is in fact the current authentic CSCA certificate.

4.1.5.2 Revocation of other Certificates

When an issuing State or organization wishes to revoke a Signer certificate issued under the CSCA, it does not need to wait until the `nextUpdate` period in the current CRL is due to issue a new CRL. It is RECOMMENDED that a new CRL be issued within a 48-hour period of revocation notification.

4.1.6 Cryptographic Algorithms

An issuing State or organization MAY support different algorithm for use in their CSCA and Signing Certificate keys. For example, the CSCA may have been issued using RSA, but Signer Certificates could be ECDSA and vice versa.

Issuing States or organizations SHALL choose appropriate key lengths offering protection against attacks. Suitable cryptographic catalogues SHOULD be taken into account.

Receiving States MUST support all algorithms at points where they wish to validate the signature on eMRTDs.

For use in their CSCA, Signing keys and, where applicable, Document Security Objects, issuing States or organizations SHALL support one of the algorithms below.

4.1.6.1 RSA

Those issuing States or organizations implementing the RSA algorithm for signature generation and verification of certificates and the Document Security Object (SO_D) SHALL use [RFC 4055]. [RFC 4055] specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED that issuing States or organizations generate signatures according to RSASSA-PSS, but receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15.

4.1.6.2 Digital Signature Algorithm (DSA)

Those issuing States or organizations implementing DSA for signature generation or verification SHALL use [FIPS 186-4].

4.1.6.3 Elliptic Curve DSA (ECDSA)

Those issuing States or organizations implementing ECDSA for signature generation or verification SHALL use [X9.62] or [ISO/IEC 15946]. The elliptic curve domain parameters used to generate the ECDSA key pair MUST be described explicitly in the parameters of the public key, i.e. parameters MUST be of type ECParameters (no named curves, no implicit parameters) and MUST include the optional co-factor. ECPoints MUST be in uncompressed format.

It is RECOMMENDED that the guideline [TR 03111] be followed.

4.1.6.4 Hashing Algorithms

SHA-224, SHA-256, SHA-384 and SHA-512, are the only permitted hashing algorithms. See [FIPS 180-2].

4.1.7 Cryptographic Algorithms for LDS2 Signer Certificates

Because LDS2 certificates and signed objects are stored on the contactless IC, they need to be as compact as possible. Therefore LDS2 Signers MUST use ECDSA, irrespective of the algorithm used in the CSCA and Document Signing keys.

4.2 Authorization PKI

Issuing States or organizations that implement LDS2 SHALL have the following key pair types:

- Country Verifying CA (CVCA) Key Pair
- Document Verifier (DV) Key Pair
- Terminal Key Pair

The CVCA and DV public keys are certified by the CVCA. The terminal public keys are certified by the DV. CVCA, DV and terminal public key certificates are card-verifiable certificates that MUST comply with their respective certificate profiles defined in Section 7. There is no revocation mechanism for CVCA, DV or terminal certificates. Therefore their validity periods are much shorter than the X.509 certificate types.

The private key usage period is not specified and is up to the discretion of the State. However, the private key usage period MUST be at most equal to the public key validity period. The public key validity period for CVCA, DV and terminal key pairs is outlined in Table 2.

Table 2. Key Usage Card-Verifiable Certificate Validity

	Public Key Validity
CVCA	6 months – 3 years
DV	2 weeks – 3 months
Terminal	1 day – 1 month

4.2.1 Cryptographic Algorithms for Terminal Authentication

The algorithm used for Terminal Authentication in the authorization PKI is determined by the CVCA of the eMRTD Issuing State. The same signature algorithm, domain parameters and key sizes MUST be used within a certificate chain (i.e. the CVCA, DV and terminal certificates for a given authorization). As a consequence Document Verifiers and terminals will have to be provided with several key pairs. CVCA Link Certificates MAY include a public key that deviates from the current parameters, i.e. the CVCA MAY switch to a new signature algorithm, new domain parameters, or key sizes.

For Terminal Authentication, either RSA or ECDSA MAY be used. Details are provided in Doc 9303-11.

4.2.2 Cryptographic Algorithms for SPOC

The TLS Encryption Suites to be used for the SPOC protocol are listed in Table 5.

Table 3. TLS Encryption Suites

Cipher Suite	**Certificate and Key Exchange Algorithm**
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA

In the scope of the TLS handshake negotiation, the client SHALL support all the TLS cipher suites defined in Table 5. Both the server and the client side SHALL support RSA and ECDSA based authentication. It is permissible for a server to request and also for the client to send a client certificate of a different type than the server certificate.

The use of the ECDHE_ECDSA key agreement in TLS handshake is in accordance with the additions defined in [TLSECC], [TLS1.2] and [TLSEXT]. Both the client and the server SHALL support the appropriate Elliptic curves extensions as specified in [TLSECC] specification in the scope of TLS handshake. The supported Elliptic curves and EC Point formats are defined in Section 5 of [TLSECC]. The use of the supported TLS cipher suites defined in Table 4 which uses Advanced Encryption Standard (AES) for encryption SHALL be in accordance with [TLSAES] specification.

5. DISTRIBUTION MECHANISMS

For eMRTD PKI, the PKI objects need to be distributed to the receiving States. A number of different distribution mechanisms are used, depending on the type of object and operational requirements. It is important to note that distribution of these objects does NOT establish trust in those objects, or the private/public keys associated with them. Mechanisms for establishing trust are specified in Section 6.1.

The distribution mechanism for the Authorization PKI is covered in Section 8.

The objects that need to be distributed from issuing States or organizations to receiving States include:

- CSCA certificates;

- CSCA Link Certificates;
- Document Signer certificates;
- LDS2 Signer certificates;
- Initial CVCA certificates;
- CVCA Link certificates;
- DV certificates;
- Bar Code Signer certificates;
- CRLs (null and non-null);
- Master List Signer certificates; Master Lists; and
- Deviation List Signer certificates; Deviation Lists.

The distribution mechanisms used in the eMRTD and Authorization PKI include:

- PKD;
- Bilateral exchange;
- SPOC;
- Master Lists;
- Deviation Lists; and
- eMRTD contactless IC.

A primary and secondary (where relevant) distribution mechanism is specified for each object as outlined in Table 6.

Table 4. Distribution of PKI Objects

	Contactless IC	***SPOC***	***Bilateral***	***PKD***	***Deviation List***	***Master List***	***Notes***
CSCA Certificates			Y (primary)			Y (Secondary)	
Document Signer Certificates	Y (primary)			Y (secondary)			Certificates written at same time SOD is written
LDS2 Signer certificates	Y						Certificates written at same time signed object is written
CVCA Initial Certificate	Y						Certificate written at eMRTD personalization time
CVCA Link Certificates	Y	Y					Certificates distributed to DVs via SPOC and CVCA Trust Anchor updated on contactless IC at next verification
DV Certificates		Y					Distributed only to subject DV

CRLs (Null and Non-null)			Y (Secondary)	Y (Primary)			CRLs issued by CSCA include revocation information relevant to LDS2 PKI objects
Master List Signer Certificates						Y	
Bar Code Signer Certificates			Y (Secondary)	Y (Primary)			Bar Code Signers are not encoded in the Bar Code and hence distribution must be ensured for validation of bar code
Master Lists			Y	Y			
Deviation List Signer Certificates					Y		

Operationally, receiving States are not obliged to use both the primary and secondary source. In the daily operation of an Inspection System, it is at the inspecting authority's discretion whether to use the primary or the secondary source. If the authority of the receiving State uses the secondary source for a certificate or CRL in its daily operations, it should be prepared to support the primary source as well.

Issuing States or organizations need to plan their key pair rollover strategies for both CSCA keys and Signer Keys in order to enable propagation of certificates and CRLs into receiving States' border control systems in a timely manner. Ideally propagation will occur within 48 hours, but some receiving States may have remote and poorly connected border outposts to which it may take more time for certificates and CRLs to propagate out. Receiving States SHOULD make every effort to distribute these certificates and CRLs to all border stations within 48 hours.

Issuing States or organizations should expect that CSCA certificates (C_{CSCA}) will be propagated by receiving States within 48 hours.

Issuing States or organizations ensure the timely propagation of Document Signer certificates (C_{DS}) by including the Document Signer certificate (C_{DS}) within the Document Security Object (SO_D). They should expect that Document Signer certificates (C_{DS}) published in the PKD will also be propagated to border stations within 48 hours.

The bar code Signer Certificates are not contained in the digital seal itself. Hence, a country that issues documents protected with digital seals MUST publish all its bar code Signer Certificates. The primary distribution channel for bar code Signer Certificates is PKD/bilateral. Other mechanisms, e.g. publication on a website, are secondary channels.

For Bar Code Signers, Publication MUST adhere to the following principles:

- As soon as a new certificate is created, it MUST be published with a delay of no more than 48 hours.
- The certificates MUST remain published until their expiration or revocation.

Receiving States SHOULD make every attempt whether electronically or by other means to act upon CRLs, including those CRLs issued under exceptional circumstances.

Timely propagation of Master List Signer certificates is ensured by including them within each Master List.

5.1 PKD Distribution Mechanism

ICAO provides a Public Key Directory (PKD) service. This service SHALL accept PKI objects, including certificates, CRLs and Master Lists, from PKD participants, store them in a directory, and make them accessible to all receiving States.

CSCA certificates (C_{CSCA}) are not stored individually as part of the ICAO PKD service. However, they may be present in the PKD if they are contained on Master Lists.

Every certificate remains in the PKD until its certificate validity period has expired, regardless of whether or not the corresponding private key is still in use.

Certificates, CRLs and Master Lists stored in the PKD by all PKD participants SHALL be made available to all parties (including non-PKD participants) that need this information for validating the authenticity and integrity of digitally stored eMRTD data, LDS2 Objects and VDS objects.

5.1.1 PKD Upload

Only PKD participants MAY upload certificates, CRLs and Master Lists to the PKD. All certificates and CRLs MUST comply with the profiles in Section 7. All Master Lists MUST comply with the specifications in Section 9.

The PKD consists of a “Write Directory” and a “Read Directory”. PKD participants SHALL use the Lightweight Directory Access Protocol (LDAP) to upload their objects to the Write Directory. Once the digital signature has been verified on an object, and other due diligence checks completed, the object is published in the Read Directory.

5.1.2 PKD Download

Read access to all certificates, CRLs and Master Lists published in the PKD SHALL be available to PKD participants and non-participants. Access control SHALL NOT be implemented for PKD read access.

It is the receiving State’s responsibility to distribute objects downloaded from the PKD to its Inspection Systems and to maintain a current CRL cache along with the certificates necessary to verify the signatures on eMRTD data.

5.2 Bilateral Exchange Distribution Mechanism

For CRLs and CSCA certificates (C_{CSCA}), the primary distribution channel is bilateral exchange between issuing States or organizations and receiving States. Bilateral exchange can also be used to distribute Master Lists.

The specific technology used for that bilateral exchange may vary depending on the policies of each issuing State or organization that has a need to distribute its certificates, CRLs and Master Lists, as well as the policies of each receiving State that needs access to those objects. Some examples of technologies that may be used in bilateral exchange include:

- diplomatic courier/pouch;
- email exchange;
- download from a website associated with the issuing CSCA; and
- download from an LDAP server associated with the issuing CSCA.

This is not an exhaustive list and other technologies may also be used.

5.3 Master List Distribution Mechanism

Master Lists are a supporting technology for the bilateral distribution scheme. As such, distribution of CSCA certificates via Master Lists is a subset of the bilateral distribution scheme.

A Master List is a digitally signed list of the CSCA certificates that are “trusted” by the receiving State or organization that issued the Master List. CSCA self-signed Root certificates and CSCA Link certificates may be included in a Master List. The structure and format of a Master List is defined in Section 8. Publication of a Master List enables other receiving States or organizations to obtain a set of CSCA certificates from a single source (the Master List issuer) rather than establish a direct bilateral exchange agreement with each of the issuing authorities or organizations represented on that list.

A Master List Signer is authorized by a CSCA to compile, digitally sign, and issue Master Lists. Master Lists MUST NOT be signed and issued directly by a CSCA itself. Master List Signer certificates MUST comply with the certificate profile defined in Section 7.

Before issuing a Master List the issuing Master List Signer SHOULD extensively validate the CSCA certificates to be countersigned, including ensuring that the certificates indeed belong to the identified CSCAs. The procedures used for this out-of-band validation SHOULD be reflected in the published certificate policies of the CSCA that issued the Master List Signer certificate.

Each Master List MUST include the Master List Signer’s certificate that will be used to verify the signature on that Master List as well as the CSCA certificates of the CSCA that issued that Master List Signer certificate.

If new CSCA certificates have been received by a receiving State, and its validation procedures have been completed, it is RECOMMENDED that a new Master List be compiled and issued.

Use of a Master List does enable more efficient distribution of CSCA certificates for some receiving States. However a receiving State making use of Master Lists MUST still determine its own policies for establishing trust in the certificates contained on that list (see Section 6 for details).

6. PKI TRUST AND VALIDATION

PKI Trust and Validation differ between the eMRTD PKI and Authorization PKI.

6.1 eMRTD PKI

In the eMRTD PKI environment, the Inspection Systems in receiving States act in the role of PKI relying parties. Successful verification of the digital signature on the Document Security Object of an eMRTD ensures the authenticity and integrity of the data stored on the contactless IC of that eMRTD. That signature verification process requires that the relying party establish that the Document Signer public key used to verify the signature is itself "trusted".

The various distribution mechanisms defined in Section 5 allow receiving States to gain access to the certificates and CRLs that they need to verify digital signatures in question. However, these distribution schemes do not establish trust in those certificates, CRLs or the public keys that will be used to verify signatures on those certificates and CRLs.

The public keys contained in CSCA certificates (C_{CSCA}) are used to verify the digital signature on certificates and CRLs. Therefore, to accept an eMRTD from another issuing State, the receiving State MUST already have placed into some form of trust store, accessible by their border control system, a trusted copy of the issuing State or organization CSCA certificate (C_{CSCA}), or other form of Trust Anchor information for that CSCA public key as derived from the certificate.

It is a receiving State's responsibility to establish trust in the CSCA certificates (C_{CSCA}) and store the certificates (or information from the certificates) as Trust Anchors, in a secure way for use by their border inspection systems.

6.1.1 Trust Anchor Management

As specified in [RFC 5280] a Trust Anchor must be established that can be used to anchor the validation procedure for a given Document Signer, Master List Signer, Deviation List Signer or other type of certificate.

Each Trust Anchor is comprised of a trusted public key and associated metadata. Trust Anchors MUST include, at a minimum:

- the trusted public key and any associated key parameters;
- the public key algorithm;
- the name of the key owner; and
- the value of the `SubjectAltName` extension of the CSCA certificate containing the ICAO assigned three-letter code of the issuing authority or organization. Although this is not used in the certification path or CRL validation procedures, it is used in Passive Authentication defined in Doc 9303-11.

In the eMRTD application, a separate Trust Anchor is established for each public key of a given CSCA. For the initial public key obtained from a CSCA, trust MUST be established through an out-of-band mechanism. For example, if a CSCA certificate was downloaded from a server associated with the CSCA, out-of-band communication (e.g. phone or email) could be used to verify that the downloaded certificate is in fact the authentic certificate for that CSCA. Also, the relying party might analyse the policies, procedures and practices of the issuing CSCA to determine whether they are secure enough to satisfy the local requirements for use of certificates. Once an initial Trust Anchor is established for a given CSCA, the process could be simplified for subsequent keys for that same CSCA. If the CSCA issues a CSCA Link certificate, then out-of-band communication with the CSCA to verify the authenticity of the new certificate could be skipped because the already trusted public key for that same CSCA is used to verify the signature on that CSCA Link certificate.

Trust Anchor information may be stored as a trusted copy of the CSCA certificate itself, or in some other trusted format.

Because signatures on certificates issued by CSCAs need to be verifiable long after that CSCA has updated its key pair, a receiving State will typically have more than one Trust Anchor for the same CSCA at any one time. If a CSCA has undergone a name change, some of these Trust Anchors will contain the old CSCA name and others will contain the new name.

6.1.2 Certificate/CRL Validation and Revocation Checking

As part of the process of verifying the authenticity and integrity of data objects in the eMRTD application (e.g. Document Security Objects, Master Lists, Deviation Lists, etc.), a Receiving State:

- validates the certificate used to verify the signature on the data object (e.g. Document Signer Certificate,

Master List Signer certificate, Deviation List Signer certificate);

- validates the CRL that is used to check the revocation status of the certificate in question; and
- processes the CRL to verify the revocation status of the certificate in question.

Sample algorithms for these processes are available, such as those specified in [RFC 5280]. Receiving States need not implement the specific algorithm defined in RFC 5280, but MUST provide functionality equivalent to the external behaviour resulting from this procedure. Any algorithm may be used by a particular implementation as long as it derives the correct result.

Appendix D provides guidance for receiving States that choose to base their algorithm on that specified in [RFC 5280].

6.1.3 Bar Code Validation Authority

The bar code Validation Authority validates a digital seal by applying a Validation Policy. Doc 9303-13 specifies in detail validation criteria and algorithms to generate a validation status.

Figure 4 illustrates the functional architecture of the bar code Validation Authority. The bar code Validation Authority relies on validation software which can be deployed on any computer used by the border control authorities.

The validation software is connected with a reader that takes an image of the bar code to retrieve the bar code and the MRZ of the document, and also, an image of the document to retrieve its MRZ. To verify the validity of the signature of the digital seal, the validation software SHOULD be synchronized with the PKI publication point at least every 24 hours to retrieve the latest bar code Signer Certificates and CRLs.

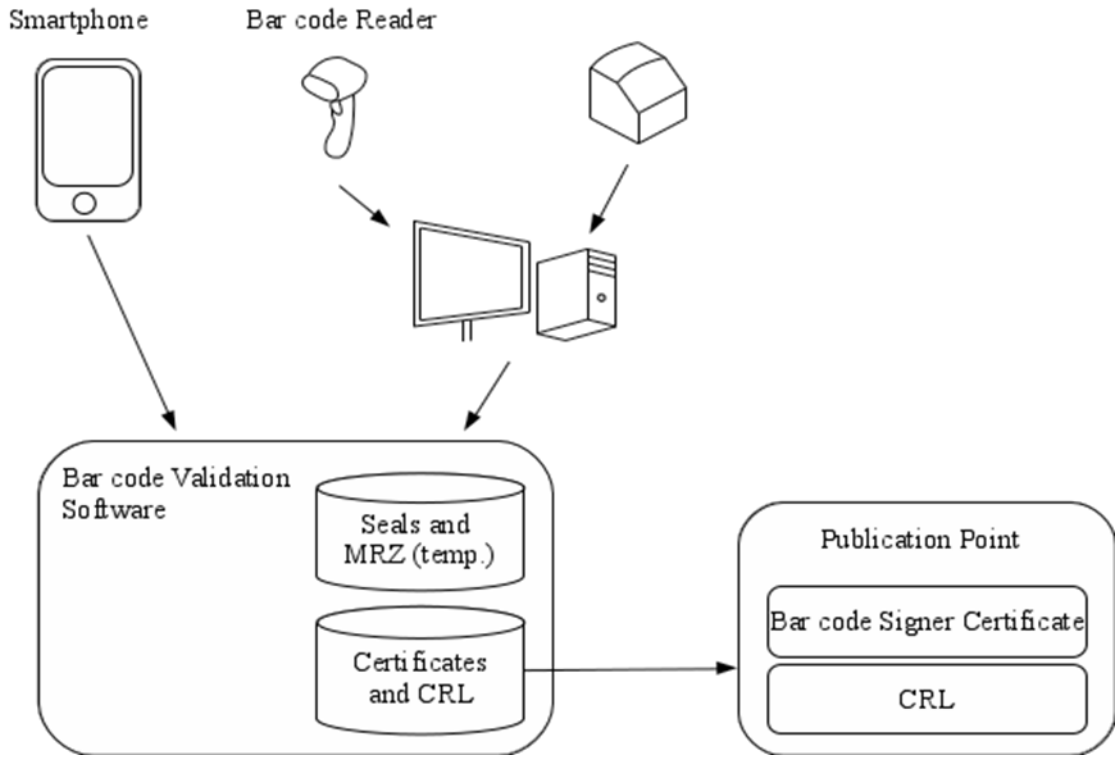


Figure 4 : Bar Code Validation

The bar code validation software decodes the digital seal and the MRZs of any associated documents (e.g. visa or passport), validates the signature of the digital seal, and applies a validation policy (cf. 9303-13) to generate a validation status of the document.

In mobile scenarios, the validation software can also be directly run on a smartphone. Whereas the validity of the seal can be verified by the software on the smartphone, the comparison between the (signed) data inside the seal and the printed MRZs (e.g. of the visa or passport) MUST be done either manually, or by OCR of the MRZs out of the captured image, the latter being often a challenging problem in practice.

The following data are processed by the bar code validation software:

- Input data provided by readers, e.g. the images of visas or passports
- Certificates and CRLs

6.2 Authorization PKI

For Authorization PKI, the Trust Anchor and Validation is handled differently.

6.2.1 Validation of Card Verifiable Certificates

For DV and terminal certificates in the authorization PKI, the Trust Anchor is the most recent public key of the CVCA of the State that issued the eMRTD. The initial Trust Anchor SHALL be stored securely in the eMRTD contactless IC in the production or (pre-) personalization phase. As the key pair used by the CVCA changes over time, CVCA Link Certificates are produced. The eMRTD contactless IC MUST internally update its Trust Anchor(s) according to received valid link certificates. Due to the scheduling of CVCA Link Certificates, at most two CVCA Trust Anchors will be stored on the contactless IC at any one time.

To validate a Terminal Certificate, the eMRTD contactless IC MUST be provided with a certificate chain starting at a Trust Anchor stored on the eMRTD contactless IC.

The validation procedure for DV and terminal certificates is specific to the LDS2 terminal authentication protocol and is specified in Doc 9303-11.

7. CERTIFICATE AND CRL PROFILES

Certificate profiles are defined for both the eMRTD PKI and the Authorization PKI.

7.1 eMRTD PKI

Issuing States or organizations MUST issue certificates and CRLs that conform to the profiles specified below. All certificates and CRLs MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them. The profiles for CSCA and DS certificates that were included in the sixth edition of this specification differ in some areas from the current profiles. Inspection Systems MUST be capable of handling certificates that were issued in accordance with those earlier profiles (see Appendix C) as well as the current profiles.

These profiles are based on the requirement that each issuing State or organization or entity SHALL create a single CSCA for the purpose of signing all Doc 9303 compliant eMRTDs.

Certificate profiles are defined in Section 7.1 for the following certificate types:

- Country Signing CA;
- Document Signer;
- CSCA Master List Signer;
- Deviation List Signer; and
- Communications – even though it is not strictly needed today. This is a future proofing step. These certificates may be used for access to the PKD or for LDAP/EMAIL/HTTP communications between States. It is recommended that these certificates be issued by the CSCA.

The Country Signing CA, Document Signer, Deviation List Signer and CSCA Master List Signer objects are defined in Section 3.

The CRL profile is defined in Section 7.1.4.

The profiles use the following terminology for presence requirements of each of the components/extensions:

m mandatory — the field MUST be present;
x do not use — the field MUST NOT be present;
o optional — the field MAY be present.
C conditional – the field SHALL be present under certain conditions

The profiles use the following terminology for criticality requirements of extensions that may/must be included:

c critical — receiving applications MUST be able to process this extension;
nc non-critical — receiving applications that do not understand this extension MAY ignore it.

Some of the requirements identified in these profiles are inherited from the referenced base profiles (e.g. RFC 5280). For convenience, the relevant text from the base profile that covers the specific requirement is duplicated in a table in Appendix B.

7.1.1 Certificate Profiles

Table 7 defines the certificate profile requirements common to all certificates for the fields of the certificate body. Table 8 defines the requirements for certificate extensions.

Table 5. Certificate Fields Profile

Certificate Component	*Presence*	*Comments*
`Certificate`	m	
`TBSCertificate`	m	See next part of the table
`signatureAlgorithm`	m	Value inserted here dependent on algorithm selected
`signatureValue`	m	Value inserted here dependent on algorithm selected
`TBSCertificate`		
`version`	m	MUST be `v3`
`serialNumber`	m	MUST be positive integer and maximum 20 Octets MUST use 2's complement encoding and be represented in the smallest number of octets
`signature`	m	Value inserted here MUST be the same as that in `signatureAlgorithm` component of `Certificate` sequence
`issuer`	m	`countryName` and `serialNumber`, if present, MUST be `PrintableString` Other attributes that have `DirectoryString` syntax MUST be either `PrintableString` or `UTF8String` `countryName` MUST be Upper Case See 7.1.1 for naming conventions
`validity`	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in `UTCTime` `UTCTime` MUST be represented as YYMMDDHHMMSSZ

Certificate Component	*Presence*	*Comments*
		Dates in 2050 and beyond MUST be in `GeneralizedTime`. `GeneralizedTime` MUST NOT have fractional seconds `GeneralizedTime` MUST be represented as YYYYMMDDHHMMSSZ
`subject`	m	`countryName` and `serialNumber`, if present, MUST be `PrintableString` Other attributes that have `DirectoryString` syntax MUST be either `PrintableString` or `UTF8String` `countryName` MUST be Upper Case `countryName` in `issuer` and `subject` fields MUST match See 7.1.1 for naming conventions
`subjectPublicKeyInfo`	m	
`issuerUniqueID`	x	
`subjectUniqueID`	x	
`extensions`	m	See next table on which extensions should be present Default values for extensions MUST NOT be encoded

Table 6. Certificate Extensions Profile

Extension name	***CSCA Self-Signed Root***		***CSCA Link***		***Document Signer***		***Master List Signer and Deviation List Signer***		***Communication***		***Comments***
	Presence	***Criticality***	***Presence***	***Criticality***	***Presence***	***Criticality***	***Presence***	***Criticality***	***Presence***	***Criticality***	
AuthorityKeyIdentifier	**o**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	
keyIdentifier	m		m		m		m		m		
authorityCertIssuer	o		o		o		o		o		
authorityCertSerialNumber	o		o		o		o		o		
SubjectKeyIdentifier	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
subjectKeyIdentifier	m		m		m		m		m		
KeyUsage	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	
digitalSignature	x		x		m		m		o		Some communication certificates (e.g. TLS certificates) require that the `keyUsage` bits be set in accordance with the particular cipher suite used. Some cipher suites do, and some do not require the `digitalSignature` bit to be set.
nonRepudiation	x		x		x		x		x		
keyEncipherment	x		x		x		x		o		
dataEncipherment	x		x		x		x		x		
keyAgreement	x		x		x		x		o		
keyCertSign	m		m		x		x		x		
cRLSign	m		m		x		x		x		
encipherOnly	x		x		x		x		x		
decipherOnly	x		x		x		x		x		
PrivateKeyUsagePeriod	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	
notBefore	o		o		o		o		o		At least one of `notBefore` or `notAfter` MUST be present MUST be encoded as `generalizedTime`
notAfter	o		o		o		o		o		
CertificatePolicies	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
PolicyInformation	m		m		m		m		m		
policyIdentifier	m		m		m		m		m		
policyQualifiers	o		o		o		o		o		
PolicyMappings	**x**		**x**		**x**		**x**		**x**		See Note 1
SubjectAltName	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	See 7.1.1.2
IssuerAltName	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	See 7.1.1.2

Extension name	CSCA Self-Signed Root		CSCA Link		Document Signer		Master List Signer and Deviation List Signer		Communication		Comments
SubjectDirectoryAttributes	**x**		**x**		**x**		**x**		**x**		
Basic Constraints	**m**	**c**	**m**	**c**	**x**		**x**		**x**		
cA	m		m		x		x		x		
PathLenConstraint	m		m		x		x		x		MUST always be '0'
NameConstraints	**x**		**x**		**x**		**x**		**x**		See Note 1
PolicyConstraints	**x**		**x**		**x**		**x**		**x**		See Note 1
ExtKeyUsage	**x**		**x**		**x**		**m**	**c**	**m**	**c**	See 7.1.1.3
CRLDistributionPoints	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	
distributionPoint	m		m		m		m		m		MUST be ldap, http or https See 7.1.1.4
reasons	x		x		x		x		x		
cRLIssuer	x		x		x		x		x		
InhibitAnyPolicy	**x**		**x**		**x**		**x**		**x**		See Note1
FreshestCRL	**x**		**x**		**x**		**x**		**x**		See Note 2
privateInternetExtensions	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	See Note 3
NameChange	**o**	**nc**	**o**	**nc**	**x**		**x**		**x**		See 7.1.1.5
DocumentType	**x**		**x**		**m**	**nc**	**x**		**x**		See 7.1.1.6
Netscape Certificate Type	**x**		**x**		**x**		**x**		**x**		See Note 4
other private extensions	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	

Note 1.— The extension, by definition, can only appear in intermediate CA certificates (certificates issued by one CA to another CA). Intermediate CA certificates are not used in the eMRTD PKI. Therefore this extension is prohibited from eMRTD certificates.

Note 2.— The freshest CRL extension is used to point to a delta CRL. Delta CRLs are not supported in the eMRTD PKI. Therefore this extension is prohibited.

Note 3.— There are two Private Internet Extensions (Authority Information Access and Subject Information Access) defined in RFC 5280 that are used to point to information about the issuer or subject of a certificate. These extensions are not required in the eMRTD PKI. However as they do not impact interoperability, and are non-critical, they may optionally be included in eMRTD certificates.

Note 4.— The Netscape Certificate Type extension can be used to limit the purposes for which a certificate can be used. The `extKeyUsage` and `basicConstraints` extensions are now the standard extensions for those purposes and are used in the eMRTD application. Because of the potential conflict between values in the standard extensions and in the Netscape proprietary extension, the Netscape extension is prohibited.

7.1.1.1 Issuer and Subject Field requirements

The Issuer and Subject Fields are common to all certificates, but specific restrictions apply for LDS2 Signer Certificates.

7.1.1.1.1 General requirements

The following naming and addressing conventions for `Issuer` and `Subject` fields are REQUIRED.

- `countryName`. MUST be present. The value contains a country code that MUST follow the format of two letter country codes, specified in Doc 9303-3.
- `commonName`. MUST be present.

Other attributes MAY also be included at the discretion of the issuing State or organization.

7.1.1.1.2 LDS2 Signer Certificate requirements

LDS2 Signer Certificates MUST comply with the Document Signer Certificate profile defined above with the exceptions defined in 7.1.2.

7.1.1.2 Issuer and Subject Alternative Name requirements

Because the functions served by alternative names in the eMRTD application are specific to this application, and different from those defined for the Internet PKI in [RFC 5280], values in the Subject Alternative Name extension of eMRTD certificates do not generally unambiguously identify the certificate subject.

In the eMRTD application, alternative names serve the following two functions.

The first function is to provide contact information for the subject and/or issuer of the certificate. For that purpose it SHOULD include at least one of the following:

- `rfc822Name`;
- `dNSName`; or
- `uniformResourceIdentifier`.

The second function is to provide a directory string made of ICAO assigned country codes. For this purpose certificates issued using this profile MUST additionally include a directory name that is constructed as follows:

- `localityName` that contains the ICAO country code as it appears in the MRZ; and
- if this country code does not uniquely define the issuing State or organization, the attribute `stateOrProvinceName` SHALL be used to indicate the ICAO assigned three-letter code for the issuing State or organization.
- Other attributes are not permitted.

In CSCA self-signed Root certificates, the `IssuerAltName` and `SubjectAltName` extensions MUST be identical. In CSCA Link certificates, the values MAY be different. For example, if a change has occurred with the `rfc822Name` of the CSCA immediately prior to issuance of a CSCA Link certificate, the `IssuerAltName` extension would contain the old `rfc822Name` and the `SubjectAltName` extension would contain the new `rfc822Name`. Any subsequent CSCA Link certificates would contain the new `rfc822Name` in both extensions.

7.1.1.3 Extended key usage extension requirements

The Object Identifier (OID) that must be included in the `extendedKeyUsage` extension for Master List Signer certificates is `2.23.136.1.1.3`.

The Object Identifier (OID) that must be included in the `extendedKeyUsage` extension for Deviation List Signer certificates is `2.23.136.1.1.8`.

For communication certificates the value of this extension depends on the communication protocol used (see RFC 5280, section 4.2.1.12).

7.1.1.4 CRL distribution points extension requirements

CSCAs may publish their CRL in several places including the PKD, their own website, etc.

For CRLs that are published in locations other than the PKD (e.g. website or local LDAP server), the values that are to be included in this extension are under the control of the CSCA issuing the certificates and the CRL in question.

For CRLs submitted to the PKD, PKD participants MAY include two URL values for their CRL using the following template (replace "CountryCode" with the issuing State or organization ICAO assigned three-letter code). If this country code does not uniquely identify the issuing State or organization, the entry will be created by appending the symbol "_" to the three-letter country code in the MRZ, and then the ICAO assigned three-letter code for the issuing State or organization which uniquely identifies the issuing State or organization:

https://pkddownload1.icao.int/CRLs/CountryCode.crl
https://pkddownload2.icao.int/CRLs/CountryCode.crl

This is a mandatory extension, and revocation status checks are a mandatory part of the validation procedure. Therefore at least one value MUST be populated.

- The PKD values may be the only values in the extension;
- There may be additional values (e.g. a CSCA may also choose to publish its CRL on a website and include a pointer to that source); or
- A CSCA may also choose to include only a single value (e.g. a pointer to its website as a source) even if it also submits its CRL to the PKD.

The following examples illustrate the PKD values that would be populated in certificates issued by the issuing authority for Singapore and for Hong Kong:

Singapore PKD example:
https://pkddownload1.icao.int/CRLs/SGP.crl
https://pkddownload2.icao.int/CRLs/SGP.crl

Hong Kong example:
https://pkddownload1.icao.int/CRLs/CHN_HKG.crl
https://pkddownload2.icao.int/CRLs/CHN_HKG.crl

7.1.1.5 Name change extension

When a CSCA key rollover occurs, a certificate MUST be issued that links the old public key to the new public key to provide a secure transition for relying parties. Generally this is achieved through the issuance of a self-issued certificate where the `issuer` and `subject` fields are identical but the key used to verify the signature represents the old key pair and the certified public key represents the new key pair.

It is RECOMMENDED that CSCAs do not change their Distinguished Name (DN) unnecessarily as there is an adverse impact on relying parties (they must retain both the old and new names as valid CSCAs for the same issuing State or organization until all eMRPs signed under the old name have expired). However, if a name change is necessary, this MUST be conveyed to relying parties through the issuance of a CSCA Link certificate where the `issuer` field contains the old name and the `subject` field contains the new name. This CSCA Link certificate also conveys a key rollover where the key used to verify the signature represents the old key pair and the certified public key represents the new key pair. Certificates that convey both a CSCA name change and a key rollover for that CSCA MUST include the `NameChange` extension to identify the certificate as such. This has no effect on `PathLengthConstraint`; it remains `'0'`.

In addition, the `NameChange` extension MAY also be included in the new CSCA self-signed certificate created upon the change of the CSCA DN. In such a self-signed CSCA Root certificate, both the `issuer` and `subject` fields contain the new

DN. Unlike the CSCA self-issued link certificate, containing both the old and new DN for the CSCA, inclusion of the `NameChange` extension in a CSCA self-signed Root certificate simply indicates that a name change has occurred and does not link the old DN to the new one.

A CSCA MUST NOT re-use certificate serial numbers. Each certificate issued by a CSCA, regardless of whether that CSCA has undergone a name change or not, MUST be unique.

ASN.1 for Name Change extension:

```
nameChange EXTENSION ::= {
   SYNTAX                NULL
   IDENTIFIED BY     id-icao-mrtd-security-extensions-nameChange}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::=
{id-icao-
mrtd-security-extensions 1}
```

7.1.1.6 Document type extension

The `DocumentType` extension MUST be used to indicate the document types, as they appear in the MRZ, that the corresponding Document Signer is allowed to produce. This extension MUST always be set to non-critical.

ASN.1 for Document Type List extension:

```
documentTypeList EXTENSION ::= {
   SYNTAX                DocumentTypeListSyntax
   IDENTIFIED BY     id-icao-mrtd-security-extensions-documentTypeList}

DocumentTypeListSyntax ::= SEQUENCE {
   version           DocumentTypeListVersion,
   docTypeList       SET OF DocumentType }

DocumentTypeListVersion ::= INTEGER {v0(0)}

-- Document Type as contained in MRZ, e.g. “P” or “ID” where a
-- single letter denotes all document types starting with that letter
DocumentType ::= PrintableString(SIZE(1..2))

id-icao-mrtd-security-extensions-documentTypeList OBJECT
IDENTIFIER ::= {id-icao-mrtd-security-extensions 2}
```

7.1.2 LDS2 Signer Certificate Profile

LDS2 Signer certificates MUST comply with the Document Signer certificate profile defined in 7.1.1 with the following exceptions:

Subject Field:
The “subject” field of LDS2 Signer certificates MUST be populated as follows:

- countryName: MUST be present. The value contains a country code that MUST follow the format of two letter country codes, specified in Doc 9303-3.
- commonName: MUST be present. The value in this attribute MUST NOT exceed 9 characters in length.
- Other attributes MUST NOT be included.

Certificate extensions:
LDS2 Signer certificates MUST contain the certificate extensions identified in Table 9 below. All other certificate extensions

MUST NOT be included.

Table 7. Mandatory Certificate Extensions for LDS2

Extension name	LDS2 Signer		Comments
	Presence	Criticality	
AuthorityKeyIdentifier	**m**	**nc**	
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
ExtKeyUsage	**m**	**c**	See note 1

Note 1: The EKU extension for each LDS2 Signer certificate type MUST be populated as indicated below. Note that a single LDS2 Signer could be authorized to sign multiple LDS2 data object types. In that case the EKU extension would contain all relevant OIDs for that signer:

id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}

- *LDS2 Travel Stamp Signer (LDS2-TS) certificates*

  id-icao-tsSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 1}

- *LDS2 Visa Signer (LDS2-V) certificates:*

  id-icao-vSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 2}

- *LDS2 Biometrics Signer (LDS2-B) certificates:*

  id-icao-bSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 3}

- *Note 2: LDS2 Signer Certificates must comply with the size restrictions imposed by EF.Certificates in Part 10.*

Although the CRL Distribution Points extension is not included in these certificates, it is mandatory that the revocation status be checked for each certificate as part of the normal validation process. The CRL issued by the CSCA that issued the certificate in question is the CRL used to verify its revocation status.

7.1.3 Bar Code Signer Certificate Profile

The bar code Signer certificates MUST comply with the LDS2 Signer certificate profile. Since bar code Signer certificates serve a different role than LDS2 certificates, their profile deviates in some respects. In particular, there are specific requirements for the subjectDN of the bar code signer certificate and the serial number, see Doc 9303-13..

Subject Field:
The subject field of Bar Code Signer Certificates must be populated as follows:

- commonName: MUST be present. MUST consist of two uppercase characters, printableString format, that uniquely define the bar code Signer within one country, and MUST match the letters 3 and 4 of the Signer Identifier in the bar code, specified in Doc 9303-13.
- countryName: MUST consist of the two letter country code (see Doc 9303-3) of the bar code Signer, uppercase characters, printableString format, and MUST match letters 1 and 2 of the Signer Identifier in the bar code , specified in Doc 9303-13.
- Other attributes MUST NOT be included.

Certificate extensions:
Bar Code Signer certificates MUST contain the certificate extensions identified in Table 10 below. All other certificate extensions MUST NOT be included.

Table 8. Allowed Extensions for Bar Code Signer Certificates

Extension name	LDS2 Signer		Comments
	Presence	**Criticality**	
AuthorityKeyIdentifier	**m**	**nc**	
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
DocumentType	**o**		This extension indicates the document type, which the bar code signer is allowed to produce
ExtKeyUsage	**m**	**c**	See note 1

Note 1: The EKU extension for each Bar Code Signer certificate type MUST be populated as indicated below.
id-icao-mrtd-security-vds OBJECT IDENTIFIER ::= {id-icao-mrtd-security 11}
id-icao-vdsSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-vds 1}

7.1.4 CRL Profile

Table 11 defines the CRL profile requirements for the fields of the CRL body. Table 12 defines the CRL profile requirements for CRL and CRL Entry extensions.

Table 9. CRL Fields Profile

Certificate List Component	***CSCA CRL***	***Comments***
`CertificateList`	m	
`tBSCertList`	m	See next part of the table
`signatureAlgorithm`	m	Value inserted here dependent on algorithm selected
`signatureValue`	m	Value inserted here dependent on algorithm selected
`tBSCertList`		
`Version`	m	MUST be `v2`
`Signature`	m	value inserted here MUST be the same as that in `signatureAlgorithm` component of `CertificateList` sequence

Certificate List Component	***CSCA CRL***	***Comments***
`Issuer`	m	`countryName` and `serialNumber`, if present, MUST be `PrintableString` Other attributes that have `DirectoryString` syntax MUST be either `PrintableString` or `UTF8String` `countryName` MUST be Upper Case
`thisUpdate`	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in `UTCTime` `UTCTime` MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in `GeneralizedTime`. `GeneralizedTime` MUST NOT have fractional seconds `GeneralizedTime` MUST be represented as YYYYMMDDHHMMSSZ
`nextUpdate`	m	MUST terminate with Zulu (Z) Seconds element MUST be present Dates through 2049 MUST be in `UTCTime` `UTCTime` MUST be represented as YYMMDDHHMMSSZ Dates in 2050 and beyond MUST be in `GeneralizedTime`. `GeneralizedTime` MUST NOT have fractional seconds `GeneralizedTime` MUST be represented as YYYYMMDDHHMMSSZ
`revokedCertificates`	c	SHALL be present if there are revoked certificates. If there are no revoked certificates it SHALL NOT be present. If present, MUST NOT be empty
`crlExtensions`	m	See next table on which extensions should be present Default values for extensions MUST NOT be encoded

Table 10. CRL and CRL Entry Extensions Profile

Extension Name	*CSCA CRL*	*Criticality*	*Comments*
CRL Extensions			
authorityKeyIdentifier	**m**	**nc**	This MUST be the same value as the subjectKeyIdentifier field in the CRL issuer's certificate.
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
issuerAlternativeName	**o**	**nc**	See Note 1
cRLNumber	**m**	**nc**	MUST be non-negative integer and maximum 20 Octets MUST use 2's complement encoding and be represented in the smallest number of octets
deltaCRLIndicator	**x**		
issuingDistributionPoint	**x**		
freshestCRL	**x**		
CRL Entry Extensions			
reasonCode	**x**		
holdInstructionCode	**x**		
invalidityDate	**x**		
certificateIssuer	**x**		
other private extensions	**o**	**nc**	

Note 1.— If a CSCA has undergone a name change, this extension MAY be included in CRLs issued following the CSCA name change. If present, the value(s) in this extension MUST be identical to the issuer *field of certificates issued by the CSCA under that previous name. Once all certificates issued under a previous CSCA name have expired, that CSCA name can be excluded from subsequent CRLs. Inspection Systems are not required to process this extension. Given that ICAO Doc 9303 dictates a single CSCA per country, the* countryName *component of the issuer field is sufficient to uniquely identify the CSCA. The latest public key of that CSCA is used to verify the signature of the CRL. Since a CSCA issues a single CRL, this CRL covers all certificates issued with that* countryName*. In addition to that mandatory check, an optional check that the* issuer *field of the certificate is equal to the* issuer *field of the CRL or one of the values of the* issuerAltName *extension in the CRL MAY also be done*.

Note 2.— It is possible that the CRL contains other revocation information, for example, concerning system operator or registration authority certificates.

7.2 Authorization PKI

The authorization PKI includes X.509 certificates for SPOC and card-verifiable certificates for CVCA, DV and terminals. This

section specifies the profiles for SPOC certificates, CVCA, DV and IS certificates. An overview of the data objects contained in card- verifiable certificates is provided, and the encoding of those objects is also covered.

7.2.1 SPOC Certificate Profile

A separate CA setup can be used to directly issue SPOC certificates with the following restrictions to the self-signed CA Certificate profile.

- CA certificate MUST conform to [RFC 5280]
- SHA-224, SHA-256, SHA-384 and SHA-512, are the only permitted hashing algorithms
- `countryName` MUST be present in the Subject field

LDS2 SPOC certificates (client and server) MUST comply with the communication certificate profile defined in section 7.1, with the following restrictions.

Issuer Field:

SPOC certificates are issued either by the CSCA or a separate CA setup specifically to issue SPOC certificates.

Subject Field:
For LDS2 SPOC certificates the subject field MUST be populated as follows:

- countryName: MUST be present. The value contains a country code that MUST follow the format of two letter country codes, specified in Doc 9303-3.
- commonName: MUST be present. For SPOC TLS client certificates, the value SHOULD be “SPOC TLS client”. For SPOC TLS server certificates, the value SHOULD be “SPOC TLS server”.
- Other attributes MAY also be included at the discretion of the issuing State or organization.

Key Usage Extensions
For SPOC certificates, the value(s) are dependent on the cipher suite used.

Subject Alternative Names Extensions
In addition to the values indicated in the communication certificate profile, SPOC TLS server certificates MUST also contain a dNSName value that is the host part of the SPOC URL.

Extended Key Usage Extensions
For SPOC client and server certificates the relevant value listed below MUST be included.

- *SPOC client certificates: OID is 2.23.136.1.1.10.1*
- *SPOC server certificates: OID is 2.23.136.1.1.10.2*

CRL Distribution Point Extensions
This extension is mandatory in SPOC client and server certificates.

7.2.2 CVCA, DV and Terminal Certificate Profiles

CVCA Link Certificates, DV Certificates, and Terminal Certificates are to be validated by ICs. Due to the computational restrictions of those chips, the certificates MUST be in a card verifiable format, (CV certificates).

The certificate format and profile specified below SHALL be used. Details on encoding values can be found in Doc 9303-11.

Table 11. CV Certificate Profile

Data Object	Certificate Presence
CV Certificate	m
Certificate Body	m
Certificate Profile Identifier	m
Certification Authority Reference	m
Public Key	m
Certificate Holder Reference	m
Certificate Holder Authorization Template	m
Certificate Effective Date	m

Certificate Expiration Date	m
Certificate Extensions	o
Signature	m

7.2.2.1 Certificate Profile Identifier

The version of the profile is indicated by the Certificate Profile Identifier. Version 1 SHALL be used and is identified by a value of 0.

7.2.2.2 Certificate Authority Reference & Certificate Holder Reference

Each CV Certificate MUST contain two public key references (a Certificate Holder Reference and a Certification Authority Reference).

The Certificate Authority Reference is a reference to the (external) public key of the Certification Authority (CVCA or DV) that SHALL be used to verify the signature of the certificate.

The Certificate Holder Reference is an identifier for the public key provided in the certificate that SHALL be used to reference this public key.

Note: As a consequence, the Certificate Authority Reference contained in a certificate MUST be equal to the Certificate Holder Reference in the corresponding certificate of the issuing Certification Authority.

The Certificate Holder Reference SHALL consist of the following concatenated elements: Country Code, Holder Mnemonic, and Sequence Number. Those elements MUST be chosen according to Table 14 and the following rules:

a) Country Code:
   - The Country Code SHALL be the Doc 9303-3 2-letter code of the certificate holder's country.

b) Holder Mnemonic:
   - The Holder Mnemonic SHALL be assigned as unique identifier as follows:
     - The Holder Mnemonic of a CVCA SHALL be assigned by the CVCA itself;
     - The Holder Mnemonic of a DV SHALL be assigned by its domestic CVCA; and
     - The Holder Mnemonic of an IS SHALL be assigned by the supervising DV.

c) Sequence Number:
   - The Sequence Number SHALL be assigned by the certificate holder;
   - The Sequence Number MUST be numeric or alphanumeric;
     - A numeric Sequence Number SHALL consists of the characters "0"…"9".
     - An alphanumeric Sequence Number SHALL consist of the characters "0"…"9" and "A"…"Z".
   - The Sequence Number MUST start with the Doc 9303-3 2-letter country code of the certifying certification authority, the remaining three characters SHALL be assigned as alphanumeric Sequence Number; and
   - The Sequence Number MAY be reset if all available Sequence Numbers are exhausted.

Table 12. Certificate Holder Reference

	Encoding	**Length**
Country Code	Doc 9303-3	2F
Holder Mnemonic	ISO/IEC 8859-1	9V
Sequence Number	ISO/IEC 8859-1	5F

7.2.2.3 Public Key

This field contains the public key being certified.

CVCA self-signed certificates MUST contain domain parameters. CVCA Link certificates MAY contain domain parameters, except in the case where domain parameters have changed. In such cases, the Link certificates MUST contain the new domain parameters.

DV and Terminal certificates MUST NOT contain domain parameters. The domain parameters of DV and terminal public keys SHALL be inherited from the respective CVCA public key.

7.2.2.4 Certificate Holder Authorization Template

The role and authorization of the certificate holder SHALL be encoded in the Certificate Holder Authorization Template. This template is a sequence that consists of the following data objects:

a) An object identifier that specifies the terminal type and the format of the template; and
b) A discretionary data object that encodes the relative authorization, i.e. the role and authorization of the certificate holder relative to the certification authority.

Specific values are defined in Doc 9303-10.

7.2.2.5 Certificate Effective Date and Certificate Expiration Date

The combination of these two dates indicate the validity period of the certificate. The Certificate Effective Date MUST be the date of the certificate generation. The certificate expiration date is the date after which the certificate expires.

7.2.2.6 Certificate Extensions (Authorization Extensions)

Authorization extensions MAY be included in CVCA, DV and terminal certificates. These extensions convey authorizations additional to those in the Certificate Holder Authorization Template in the certificate.

An authorization extension is a sequence of discretionary data templates, where every discretionary data template SHALL contain a sequence of the following data objects also shown in Table 15:

a) An object identifier that specifies the content and the format of the extension; and
b) A context specific data object that contains the encoded authorization.

Table 13. Certificate Extensions

Data Object
Certificate Extensions
Discretionary Data Template
Object Identifier
Context Specific Data Object
Discretionary Data Template
Object Identifier
Context Specific Data Object
…

Note: The certificate validation procedure described in Doc 9303-11 does not take certificate extensions into account. Thus, extensions are uncritical attributes and the IC MUST NOT reject certificates due to unknown extensions.

7.2.2.7 Signature

The signature on the certificate SHALL be created over the encoded certificate body (i.e. including tag and length). The Certification Authority Reference SHALL identify the public key to be used to verify the signature.

7.2.3 Data Objects

An overview of the tags, lengths and values of the data objects used in CVCA, DV and terminal certificates is provided in Table 16.

Table 14. Overview of Data Objects (sorted by tag)

Name	***Tag***	***Len***	***Value***	***Comment***
Object Identifier	0x06	V	Object Identifier	–
Certification Authority Reference	0x42	16V	Character String	Identifies the public key of the issuing certification authority in a certificate.
Discretionary Data	0x53	V	Octet String	Contains arbitrary data.
Certificate Holder Reference	0x5F20	16V	Character String	Associates the public key contained in a certificate with an identifier.
Certificate Expiration Date	0x5F24	6F	Date	The date after which the certificate expires.

Certificate Effective Date	0x5F25	6F	Date	The date of the certificate generation.
Certificate Profile Identifier	0x5F29	1F	Unsigned Integer	Version of the certificate and certificate request format.
Signature	0x5F37	V	Octet String	Digital signature produced by an asymmetric cryptographic algorithm.
Certificate Extensions	0x65	V	Sequence	Nests certificate extensions.
Authentication	0x67	V	Sequence	Contains authentication related data objects.
Discretionary Data Template	0x73	V	Sequence	Nests arbitrary data objects.
CV Certificate	0x7F21	V	Sequence	Nests certificate body and signature.
Public Key	0x7F49	V	Sequence	Nests the public key value and the domain parameters.
Certificate Holder Authorization Template	0x7F4C	V	Sequence	Encodes the role of the certificate holder (i.e. CVCA, DV, Terminal) and assigns read/write access rights.
Certificate Body	0x7F4E	V	Sequence	Nests data objects of the certificate body.

F: fixed length (exact number of octets), V: variable length (up to number of octets)

7.2.3.1 Encoding of Values

The basic value types used in this specification are the following: (unsigned) integers, elliptic curve points, dates, character strings, octet strings, object identifiers, and sequences.

7.2.3.1.1 Unsigned Integers

All integers used in this specification are unsigned integers. An unsigned integer SHALL be converted to an octet string using the binary representation of the integer in big-endian format. The minimum number of octets SHALL be used, i.e. leading octets of value 0x00 MUST NOT be used.

Note: In contrast the ASN.1 type INTEGER is always a signed integer.

7.2.3.1.2 Elliptic Curve Points

The conversion of Elliptic Curve Points to octet strings is specified in [TR-03111]. The uncompressed format SHALL be used.

7.2.3.1.3 Dates

A date is encoded in 6 digits d1⋯d6 in the format YYMMDD using timezone GMT. It is converted to an octet string o1⋯o6 by encoding each digit dj to an octet oj as unpacked BCDs ($1 \leqslant j \leqslant 6$).

The year YY is encoded in two digits and to be interpreted as 20YY, i.e. the year is in the range of 2000 to 2099.

7.2.3.1.4 Character Strings

A character string c1⋯cn is a concatenation of n characters cj with $1 \leqslant j \leqslant n$. It SHALL be converted to an octet string o1⋯on by converting each character cj to an octet oj using the ISO/IEC 8859-1 character set.

The character codes 0x00-0x1F and 0x7F-0x9F are unassigned and MUST NOT be used. The conversion of an octet to an unassigned character SHALL result in an error.

7.2.3.1.5 Octet Strings

An octet string o1⋯on is a concatenation of n octets oj with $1 \leqslant j \leqslant n$. Every octet oj consists of 8 bits.

7.2.3.1.6 Object Identifiers

An object identifier i1.i2.⋯.in is encoded as an ordered list of n unsigned integers ij with $1 \leqslant j \leqslant n$. It SHALL be converted to an octet string o1⋯on−1 using the following procedure:

1) The first two integers i1 and i2 are packed into a single integer i that is then converted to the octet string o1. The value i is calculated as follows:

$$i=i1 \cdot 40+i2$$

2) The remaining integers ij are directly converted to octet strings oj−1 with 3 ⩽ j ⩽ n.
More details on the encoding can be found in [X.690].

Note: The unsigned integers are encoded as octet strings using the big-endian format as described in Doc 9303-11, however only bits 1-7 of each octet are used. Bit 8 (the leftmost bit) set to one is used to indicate that this octet is not the last octet in the string.

7.2.3.1.7 Sequences

A sequence D1⋯Dn is an ordered list of n data objects Dj with 1 ⩽ j ⩽ n. The sequence SHALL be converted to a concatenated list of octet strings O1⋯On by DER encoding each data object Dj to an octet string Oj.

7.2.3.2 Encoding of Public Key Data Objects

A public key data object contains a sequence of an object identifier and several context specific data objects:

- The object identifier is application specific and refers not only to the public key format (i.e. the context specific data objects) but also to its usage.
- The context specific data objects are defined by the object identifier and contain the public key value and the domain parameters.

The format of public keys data objects used in this specification is described below.

7.2.3.2.1 RSA Public Keys

The data objects contained in an RSA public key are shown in Table 17. The order of the data objects is fixed.

Table 15. RSA Public Key

Data Object	*Abbrev*	*Tag*	*Type*	*CV Certificate*
Object Identifier		0x06	Object Identifier	m
Composite Modulus	n	0x81	Unsigned Integer	m
Public Exponent	e	0x82	Unsigned Integer	m

7.2.3.2.2 Elliptic Curve Public Keys

The data objects contained in an EC public key are shown in Table 18. The order of the data objects is fixed, CONDITIONAL domain parameters MUST be either all present, except the cofactor, or all absent as follows:

- Self-signed CVCA Certificates SHALL contain domain parameters.
- CVCA Link Certificates MAY contain domain parameters.
- DV and Terminal Certificates MUST NOT contain domain parameters. The domain parameters of DV and terminal public keys SHALL be inherited from the respective CVCA public key.
- Certificate Requests MUST always contain domain parameters.

Table 16. EC Public Key

Data Object	*Abbrev*	*Tag*	*Type*	*CV Certificate*
Object Identifier		0x06	Object Identifier	m
Prime Modulus	p	0x81	Unsigned Integer	c
First coefficient	a	0x82	Unsigned Integer	c
Second coefficient	b	0x83	Unsigned Integer	c
Base point	G	0x84	Elliptic Curve Point	c
Order of the point	r	0x85	Unsigned Integer	c
Public point	Y	0x86	Elliptic Curve Point	m
Cofactor	f	0x87	Unsigned Integer	c

8. SPOC PROTOCOL

Single Point of Contact (SPOC) is the only interface exposed by a State for key management operations with foreign States for the LDS2 authorization PKI. The SPOC protocol is the key management protocol for operations between CVCAs and DVs in different States. Although the SPOC protocol MAY also be used for domestic communications between a CVCA and its domestic DVs and between a DV and the set of domestic terminals it manages, this is not required. Other key management protocols can be used for domestic key management.

The SPOC protocol is used to exchange keys and certificates, in order that:

- A DV can send a certification request to the foreign CVCA;
- A CVCA can send the issued certificate to the requesting DV;
- CVCAs and DVs can request the set of valid certificates from a foreign CVCA; and
- General messages can be exchanged between DVs and CVCAs.

Within a State:

- The CVCA SHALL utilize its domestic SPOC to accept incoming foreign certification requests and to send the resulting certificates or failure notifications to the requestor;
- DVs SHALL utilize their domestic SPOC to send certification requests to foreign CVCAs and to receive the resulting certificates or failure notifications;
- The SPOC MUST collect requests and responses from the domestic CVCA and DVs and forward them to the SPOC of the recipient State; and
- The SPOC MUST collect requests and responses from the SPOCs of other States and deliver them to the relevant domestic CVCA/DV.

The SPOC web-service communication SHALL use HTTPS with TLS authentication of both client and server.

Note: The SPOCs are communication hubs between the entities of the Authorization PKI which therefore should be available 24/7 and should be accessible by foreign SPOCs.

Each SPOC registers separately with all other SPOCs of interest, providing at least the following information:

- SPOC State – the State for which the SPOC provides the communication interface;
- SPOC URL – URL of WSDL describing SPOC interface and service location; and
- SPOC CA certificate – certificate(s) used to verify SPOC communication certificates.

8.1 SPOC Related Structures

The following structures are defined for use in SPOC messages.

8.1.1 Certificate Request Structure

Certificate requests are reduced card-verifiable certificates that may carry an additional signature. The certificate request profile specified in Table 19 SHALL be used.

Table 17. CV Certificate Request Profile

Data Object	Certificate Presence
Authentication	c
CV Certificate	m
Certificate Body	m
Certificate Profile Identifier	m
Certification Authority Reference	r
Public Key	m
Certificate Holder Reference	m
Signature	m
Certification Authority Reference	c
Signature	c

8.1.1.1 Certificate Profile Identifier

The version is version 1, identified by a value of 0.

8.1.1.2 Certification Authority Reference

The Certification Authority Reference SHOULD be used to inform the certification authority about the private key that is expected by the applicant to be used to sign the certificate. If the Certification Authority Reference contained in the request deviates from the Certification Authority Reference contained in the issued certificate (i.e. the issued certificate is signed by a private key that is not expected by the applicant), the corresponding certificate of the certification authority SHOULD also be provided to the applicant in response.

8.1.1.3 Public Key

Certificate Requests MUST always contain domain parameters.

8.1.1.4 Certificate Holder Reference

The Certificate Holder Reference is used to identify the public key contained in the request and the resulting certificate.

8.1.1.5 Signature(s)

A certificate request may have up to two signatures, an inner signature and an outer signature:

Inner Signature (REQUIRED)

The certificate body is self-signed, i.e. the inner signature SHALL be verifiable with the public key contained in the certificate request. The signature SHALL be created over the encoded certificate body (i.e. including tag and length).

Outer Signature (CONDITIONAL)

- The signature is OPTIONAL if an entity applies for the initial certificate. In this case the request MAY be additionally signed by another entity trusted by the receiving certification authority (e.g. the national CVCA may authenticate the request of a DV sent to a foreign CVCA).

- The signature is REQUIRED if an entity applies for a successive certificate. In this case the request MUST be additionally signed by the applicant using a recent key pair previously registered with the receiving certification authority.

If the outer signature is used, an authentication data object SHALL be used to nest the CV Certificate (Request), the Certification Authority Reference and the additional signature. The Certification Authority Reference SHALL identify the public key to be used to verify the additional signature. The signature SHALL be created over the concatenation of the encoded CV Certificate and the encoded Certification Authority Reference (i.e. both including tag and length).

8.2 SPOC Protocol Messages

This section details the messages used in the SPOC protocol

8.2.1 Request Certificate Message

Intended Use:

The RequestCertificate message is used by a SPOC for requesting the generation of a new certificate for one of its DVs from a foreign CVCA.

Input Parameters:

callerID: (Mandatory)

This parameter contains the identifier of the request originating State. The value SHALL be the 2 letter country code according to Doc 9303-3 2-letter code. The value of callerID SHALL be verified by the recipient SPOC with the value recorded from the originating SPOC during its registration.

messageID: (Mandatory)

This parameter contains the identification of the message. It MUST identify the message uniquely within all messages from that originator. If a response message will be sent to the originator as a result of this message, the response message will contain the same messageID. Hence an incoming response message can be assigned to the correct original message. Construction

and allocation of the messageID can be decided by the originator and is not verified by the receiving party.

certReq: (Mandatory)
This parameter contains the actual certificate request. It MUST be constructed according to Section 8.1.1.The coding MUST follow the specifications in Section 7.2.3.1.

Output Parameters:

CertificateSeq: (Conditional)
This parameter will contain the result (one or more certificates) after processing this message, if the message has been processed successfully and synchronously by the receiver. It is REQUIRED if certificates have to be sent with the response. It MUST be absent if no certificates will be sent with the message.

Return Codes:
ok_cert_available: The message has been processed successfully and synchronously. The output parameter certificateSeq contains one or more certificates.

ok_reception_ack: The reception of the message is acknowledged. No further verification of the message has been done yet. The processing of the message will be done asynchronously. The result of the processing will be sent to the registered URL using the message SendCertificates.

failure_inner_signature: The verification of the inner signature of the actual certificate request failed. failure_outer_signature: The verification of the outer signature of the actual certificate request failed. failure_syntax: The message is syntactically not correct.
failure_request_not_accepted: The message has been processed correctly but the request has not been accepted.

failure_request_syntax: The certificate request is not correct (e.g. syntax or file format) failure_expired: The certificate to be used to verify the outer signature of the request is expired.
failure_domain_parameters: The domain parameters contained in the request do not match the domain parameters of the CVCA certificate intended to sign the requested DV certificate.

failure_internal_error: Error other than above.

Remarks:
The body of the certificate request SHOULD contain a Certification Authority Reference (CAR) to inform the CVCA which private key the requestor expects will be used to sign the certificate. If the CAR in the request differs from the CAR in the issued certificate, the corresponding certificate of the CVCA SHALL also be provided in the response. In such a case, and if the message is processed synchronously, the CVCA certificate SHALL be part of the certificateSeq output parameter. The DV certificate SHALL be the first certificate in the sequence. CVCA certificates (root and/or link) SHALL be ordered by effective date (ascending) in the sequence.

8.2.2 Send Certificates Message

Intended Use:

The SendCertificates message is used by a SPOC to send the new certificate or certificate chain to the requesting SPOC. This message SHALL be generated in response to:

- RequestCertificate: upon successful asynchronous request processing after the certificate is issued
- GetCACertificates

In addition the message MUST be used when a new certificate is created (CVCA root and link) to push the certificates to registered foreign SPOC.

Input Parameters:

callerID: (Mandatory)

This parameter contains the identifier of the originating State. The value SHALL be the 2 letter country code according to Doc 9303-3 2-letter code. The value of callerID SHALL be verified by the recipient SPOC with the value recorded from the

originating SPOC during its registration.

messageID: (Conditional)
When the message is generated in response to a request message the parameter MUST contain the same value as the messageID parameter of the request message. When the message generation was triggered without external intervention (CVCA certificate rekey). The statusInfo value SHALL be new_cert_available_notification and the messageID parameter MAY be omitted and SHALL be ignored when present.

statusInfo: (Mandatory)
This parameter contains a status code about the result of processing the corresponding message. The following statuses are possible:

- new_cert_available_notification: The originating SPOC wants to notify that new CVCA certificate(s) are available without being requested.
- ok_cert_available: The request has been processed successfully. The input parameter certificateSeq contains one or more certificates.
- failure_inner_signature: The verification of the inner signature of the actual certificate request failed.
- failure_outer_signature: The verification of the outer signature of the actual certificate request failed.
- failure_syntax: The corresponding message is syntactically not correct.
- failure_request_not_accepted: The corresponding message has been processed correctly but the request has not been accepted.
- failure_certificate: One or more of the certificates sent is not correct (syntax or signature).
- failure_internal_error: error other than above certificateSeq: (Conditional).

This parameter is REQUIRED if certificates have to be sent with the message. It MUST be absent if no certificates will be sent with the message. The certificates SHALL be binary TLV DER encoded as defined in Section 7.2.3.

When the message is generated in response to a GetCACertificates message, or because there is a new certificate, the sequence SHALL contain a list of CA certificates. The list SHALL be ordered. CVCA certificates (link and/or root) SHALL be ordered by effective date in the sequence. When the sequence contains certificates with different domain parameters at least one certificate with domain parameters included for each domain parameters variant SHALL be present. All current CA certificates SHALL be included.

When the message is generated in response to RequestCertificate message the content of the sequence is the same as described for synchronous response of RequestCertificate.

Output Parameters:
None

Return Codes:

- ok_received_correctly: The message has been received correctly.
- failure_syntax: The message is syntactically not correct.
- failure_messageID_unknown: The contained messageID cannot be matched with a message formerly sent.
- failure_internal_error: Error other than above

8.2.3 Get CA Certificates Message

Intended Use:

This message is sent by a SPOC to a foreign SPOC in order to get all valid CVCA certificates (link certificates and self-signed certificates) of that State.

Input Parameters:

callerID: (Mandatory)
This parameter contains the identifier of the originating State. The value SHALL be the 2 letter country code according to Doc 9303-3 2-letter code. The value of callerID SHALL be verified by the recipient SPOC with the value recorded from the originating SPOC during its registration.

messageID: (Mandatory)
This parameter contains the identification of the message. It MUST identify the message uniquely within all messages of the originator. If a response message will be send to the originator as a result of this message, the response message will contain the same messageID. Hence an incoming response message can be assigned to the correct original message. Construction and allocation of the messageID can be decided by the originator.

Output Parameters:

certificateSeq: (Conditional)
This parameter will contain the result (one or more certificates) after processing this message, if the message has been processed successfully and synchronously by the receiver. It is REQUIRED if certificates have to be sent with the response. It MUST be absent if no certificates will be sent with the message.

Return Codes:

- ok_cert_available: The message has been processed successfully and synchronously. The output parameter certificateSeq contains one or more CA certificates.
- ok_reception_ack: The reception of the message is acknowledged. No further verification of the message has been done yet. The processing of the message will be done asynchronously. The result of the processing will be sent to the registered URL using the message SendCertificates.
- failure_syntax: The message is syntactically not correct.
- failure_internal_error: Error other than above.

Remarks:
If the message is processed successfully and accepted the CVCA MUST send all valid CVCA certificates within the response, either in the output parameter certificateSeq (synchronous processing) or in the corresponding response message SendCertificates (asynchronous processing).

8.2.4 General Messages

Intended Use:

This message is sent by a SPOC to a foreign SPOC in order to send notification or other general text human readable message.

Input Parameters:

callerID: (Mandatory)
This parameter contains the identifier of the originating State. The value SHALL be the 2 letter country code according to Doc 9303-3 2-letter code. The value of callerID SHALL be verified by the recipient SPOC with the value recorded from the originating SPOC during its registration, including message security features (digital signature certificate/TLS client certificate is registered for respective State).

messageID: (Mandatory)

This parameter contains the identification of the message. It MUST identify the message uniquely within all messages of the originator. If a response message will be send to the originator as a result of this message, the response message will contain the same messageID. Hence an incoming response message can be assigned to the correct original message. Construction and allocation of the messageID can be decided by the originator.

subject: (Mandatory)
This parameter contains the subject of the message. The subject SHOULD briefly describe the content of the message body. English MUST be used for subject.

body: (Mandatory)
This parameter contains the body of the message. The body SHALL be human readable plain text which is not intended for direct automated processing. English MUST be used for the body.

Return Codes:

- ok: The message has been accepted for delivery.
- failure_syntax: The message is syntactically not correct.
- failure_internal_error: Error other than above.

8.3 Web Service

The web service interface is the interface for the routine inter-SPOC wire data exchange. The interface SHALL use [SOAP] over [HTTPS] protocol. The SPOC web service interface SHALL conform to the WSDL specified in Section 8.3.3.

8.3.1 SOAP usage

Pure [SOAP] over [HTTPS] SHALL be used to implement the Web-service interfaces. Any other SOAP extensions (e.g. WS-Addressing, WS-Security, WS-Secure Conversation, WS-Authorization, WS-Federation, WSAuthorization, WS-Policy, WS-Trust, WS-Privacy, WS-Test and other extensions of WS) SHALL NOT be used.

The intermediary SOAP node type SHALL NOT be used. Only a direct client SPOC to server SPOC configuration SHALL be used.

The SOAP fault element SHALL be used only when a transport layer processing error that is not covered by this specification occurs. Application level errors SHALL be communicated as normal SOAP responses using the error mechanism as described for each message.

It is RECOMMENDED that the web service interface is implemented in accordance to [WS-IBP] and [WSI-SSBP].

The SPOC SOAP interface MUST conform to WSDL definition as described in Section 8.3.3.

8.3.2 Security Considerations

The SPOC web service communication SHALL use a secure and authenticated channel. SOAP over HTTPS SHALL be used. TLS v1.2 SHALL be used.

The TLS client SHALL perform following verifications:

- The server certificate SHALL be fully validated according to [RFC5280] including revocation status.
- The server certificate ExtKeyUsage extension MUST be present and SHALL contain the OIDs according to Section 7.2.1 SPOC TLS server certificate.
- The server certificate subject country SHALL be equal to the value of callerID parameter In case of any failure the TLS client MUST close the connection.

The TLS server SHALL perform following verifications:

- The client SHALL be fully authenticated using a certificate.
- The client certificate SHALL be fully validated according to [RFC5280] including revocation status.
- The client certificate ExtKeyUsage extension MUST be present and SHALL contain the OIDs according to

Section 7.2.1 SPOC TLS client certificate.

- The client certificate subject country SHALL correspond to the intended one.

In case some of the verifications fail the request SHALL be rejected using HTTP 401 Unauthorized response code.

In the scope of the TLS handshake negotiation the client SHALL support all the TLS cipher suites defined in Section 4.2.2. Both the server and the client side SHALL support RSA and ECDSA based authentication. It is permissible for a server to request and also for the client to send a client certificate of a different type than the server certificate.

The use of the ECDHE_ECDSA key agreement in TLS handshake is in accordance with the additions defined in [TLSECC], [TLS1.2] and [TLSEXT]. Both the client and the server SHALL support the appropriate Elliptic curves extensions as specified in [TLSECC] specification in the scope of TLS handshake. The supported Elliptic curves and EC Point formats are defined in Section 5 of [TLSECC]. The use of the supported TLS cipher suites defined in Section 4.2.2 which uses Advanced Encryption Standard (AES) for encryption SHALL be in accordance with the [TLSAES] specification.

8.3.3 WSDL for SPOC Web Service Interface

The SPOC SOAP interface MUST conform to the following WSDL definition:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:SPOC="http://namespaces.icao.int/lds2"
  targetNamespace="http://namespaces. icao.int/lds2">

  <wsdl:types>
    <xs:schema xmlns="http://namespaces.icao.int/lds2"
      targetNamespace="http://namespaces."
      elementFormDefault="qualified" attributeFormDefault="unqualified">
      <xs:element name="certificateSequence">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="certificate" type="xs:base64Binary" minOccurs="1"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="RequestCertificateRequest">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="callerID" type="xs:string"/>
            <xs:element name="messageID" type="xs:string"/>
            <xs:element name="certificateRequest" type="xs:base64Binary"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="RequestCertificateResponse">
        <xs:complexType>
          <xs:sequence>
            <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
            <xs:element name="result">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="ok_cert_available"/>
                  <xs:enumeration value="ok_reception_ack"/>
                  <xs:enumeration value="failure_inner_signature"/>
                  <xs:enumeration value="failure_outer_signature"/>
                  <xs:enumeration value="failure_syntax"/>
                  <xs:enumeration value="failure_request_not_accepted"/>
```

```
            <xs:enumeration value="failure_request_syntax"/>
            <xs:enumeration value="failure_expired"/>
            <xs:enumeration value="failure_domain_parameters"/>
            <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="SendCertificatesRequest">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="callerID" type="xs:string"/>
      <xs:element name="messageID" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
      <xs:element name="statusInfo">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="new_cert_available_notification"/>
            <xs:enumeration value="ok_cert_available"/>
            <xs:enumeration value="failure_inner_signature"/>
            <xs:enumeration value="failure_outer_signature"/>
            <xs:enumeration value="failure_syntax"/>
            <xs:enumeration value="failure_request_not_accepted"/>
            <xs:enumeration value="failure_certificate"/>
            <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="SendCertificatesResponse">
  <xs:complexType>
      <xs:sequence>
      <xs:element name="result">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="ok_received_correctly"/>
            <xs:enumeration value="failure_syntax"/>
            <xs:enumeration value="failure_messageID_unknown"/>
            <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="GetCACertificatesRequest">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="callerID" type="xs:string"/>
      <xs:element name="messageID" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="GetCACertificatesResponse">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
```

```
            <xs:element name="result">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="ok_cert_available"/>
                  <xs:enumeration value="ok_reception_ack"/>
                  <xs:enumeration value="failure_syntax"/>
                  <xs:enumeration value="failure_internal_error"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="GeneralMessageRequest">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="callerID" type="xs:string"/>
            <xs:element name="messageID" type="xs:string"/>
            <xs:element name="subject" type="xs:string"/>
            <xs:element name="body" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="GeneralMessageResponse">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="result">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="ok"/>
                  <xs:enumeration value="failure_syntax"/>
                  <xs:enumeration value="failure_internal_error"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:schema>
  </wsdl:types>

  <wsdl:message name="RequestCertificateRequest">
    <wsdl:part name="RequestCertificateRequest" element="SPOC:RequestCertificateRequest"/>
  </wsdl:message>
  <wsdl:message name="RequestCertificateResponse">
    <wsdl:part name="RequestCertificateResponse" element="SPOC:RequestCertificateResponse"/>
  </wsdl:message>

  <wsdl:message name="SendCertificatesRequest">
    <wsdl:part name="SendCertificatesRequest" element="SPOC:SendCertificatesRequest"/>
  </wsdl:message>
  <wsdl:message name="SendCertificatesResponse">
    <wsdl:part name="SendCertificatesResponse" element="SPOC:SendCertificatesResponse"/>
  </wsdl:message>

  <wsdl:message name="GetCACertificatesRequest">
    <wsdl:part name="GetCACertificatesRequest" element="SPOC:GetCACertificatesRequest"/>
  </wsdl:message>
  <wsdl:message name="GetCACertificatesResponse">
    <wsdl:part name="GetCACertificatesResponse" element="SPOC:GetCACertificatesResponse"/>
  </wsdl:message>
```

```
<wsdl:message name="GeneralMessageRequest">
  <wsdl:part name="GeneralMessageRequest" element="SPOC:GeneralMessageRequest"/>
</wsdl:message>
<wsdl:message name="GeneralMessageResponse">
  <wsdl:part name="GeneralMessageResponse" element="SPOC:GeneralMessageResponse"/>
</wsdl:message>

<wsdl:portType name="SPOCPortType">
  <wsdl:operation name="RequestCertificate">
    <wsdl:input message="SPOC:RequestCertificateRequest"/>
    <wsdl:output message="SPOC:RequestCertificateResponse"/>
  </wsdl:operation>
  <wsdl:operation name="SendCertificates">
    <wsdl:input message="SPOC:SendCertificatesRequest"/>
    <wsdl:output message="SPOC:SendCertificatesResponse"/>
  </wsdl:operation>
  <wsdl:operation name="GetCACertificates">
    <wsdl:input message="SPOC:GetCACertificatesRequest"/>
    <wsdl:output message="SPOC:GetCACertificatesResponse"/>
  </wsdl:operation>
  <wsdl:operation name="GeneralMessage">
    <wsdl:input message="SPOC:GeneralMessageRequest"/>
    <wsdl:output message="SPOC:GeneralMessageResponse"/>
  </wsdl:operation>
</wsdl:portType>

<wsdl:binding name="SPOCSOAPBinding" type="SPOC:SPOCPortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="RequestCertificate">
    <soap:operation soapAction="RequestCertificate"/>
    <wsdl:input>
      <soap:body parts="RequestCertificateRequest" use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body parts="RequestCertificateResponse" use="literal"/>
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="SendCertificates">
    <soap:operation soapAction="SendCertificates"/>
    <wsdl:input>
      <soap:body parts="SendCertificatesRequest" use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body parts="SendCertificatesResponse" use="literal"/>
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="GetCACertificates">
    <soap:operation soapAction="GetCACertificates"/>
    <wsdl:input>
      <soap:body parts="GetCACertificatesRequest" use="literal"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body parts="GetCACertificatesResponse" use="literal"/>
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="GeneralMessage">
    <soap:operation soapAction="GeneralMessage"/>
    <wsdl:input>
      <soap:body parts="GeneralMessageRequest" use="literal"/>
    </wsdl:input>
    <wsdl:output>
```

```
        <soap:body parts="GeneralMessageResponse" use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>

  <wsdl:service name="SPOC">
    <wsdl:port name="SPOCPort" binding="SPOC:SPOCSOAPBinding">
      <soap:address location="http://spoc-server/SPOC"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

9. CSCA MASTER LIST STRUCTURE

Master Lists are implemented as instances of the `ContentInfo` Type, as specified in [RFC 5652]. The `ContentInfo` MUST contain a single instance of the `SignedData` Type as profiled below. No other data types are included in the `ContentInfo`. All Master Lists MUST be produced in DER format to preserve the integrity of the signatures within them.

9.1 SignedData Type

The processing rules in [RFC 5652] apply.

The specification of Master List structure uses the following terminology for presence requirements of each field.

- m mandatory — the field MUST be present
- r recommended — the field SHOULD be present
- x do not use — the field MUST NOT be present
- o optional — the field MAY be present.

Table 18. Master List

Value		*Comments*
`SignedData`		
`Version`	m	Value = `v3`
`digestAlgorithms`	m	
`encapContentInfo`	m	
`eContentType`	m	`id-icao-cscaMasterList`
`eContent`	m	The encoded contents of an `cscaMasterList`
`Certificates`	m	The Master List Signer certificate MUST be included and the CSCA certificate, which can be used to verify the signature in the `signerInfos` field SHOULD be included.
`Crls`	x	
`signerInfos`	m	It is RECOMMENDED that States only provide 1 `signerinfo` within this field.

Value		***Comments***
SignerInfo	m	
Version	m	The value of this field is dictated by the `sid` field. See [RFC 5652] for rules regarding this field.
Sid	m	
subjectKeyIdentifier	r	It is RECOMMENDED that this field be supported rather than `issuerandSerialNumber`.
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over `encapsulatedContent` and `SignedAttrs`. See Note 1.
signedAttrs	m	Additional attributes may be included. However these do not have to be processed by Receiving States except to verify the signature value. `signedAttrs` MUST include signing time (see [PKCS #9]).
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters. See Note 1.
signature	m	The result of the signature generation process.
unsignedAttrs	o	Although this field MAY be included, Receiving States may choose to ignore it.

Note 1.— `DigestAlgorithmIdentifiers` MUST omit "`NULL`" parameters, while the `SignatureAlgorithmIdentifier` (as defined in RFC 3447) MUST include `NULL` as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept `DigestAlgorithmIdentifiers` with both conditions, absent parameters or with `NULL` parameters.

9.2 ASN.1 Master List Specification

```
CscaMasterList
{ joint-iso-itu-t(2) international-organization(23) icao(136) mrtd(1)
security(1) masterlist(2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

 -- Imports from RFC 5280 [PROFILE], Appendix A.1
     Certificate
```

```
       FROM PKIX1Explicit88
         { iso(1) identified-organization(3) dod(6)
           internet(1) security(5) mechanisms(5) pkix(7)
             mod(0) pkix1-explicit(18) };
-- CSCA Master List

CscaMasterListVersion ::= INTEGER {v0(0)}

CscaMasterList ::= SEQUENCE {
  version            CscaMasterListVersion,
  certList           SET OF Certificate }

-- Object Identifiers

id-icao-cscaMasterList OBJECT IDENTIFIER ::=
                                 {id-icao-mrtd-security 2}
id-icao-cscaMasterListSigningKey OBJECT IDENTIFIER ::=
                                 {id-icao-mrtd-security 3}
END
```

10. DEVIATION LIST STRUCTURE

The Deviation List is implemented as a SignedData type, as specified in [RFC 3852]. All Deviation Lists MUST be produced in DER format to preserve the integrity of the signatures within them.

The range of deviations will be bounded by:

- date range (including both the issue and expiry date);
- issuer name and serial number;
- Subject Key Identifier of DSC;
- list of eMRTD numbers.

Appropriate combinations of these values will be used to accurately bind the range of MRTDs affected. When combining values, they are to be processed as joined by “AND”. There is no option to process values as joined using “OR”.

10.1 SignedData Type

The processing rules in [RFC 3852] apply.

m mandatory – the field MUST be present.
r recommended – the field SHOULD be present.
x do not use – the field MUST NOT be populated.
o optional – the field MAY be present.

Value		*Comments*
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-DeviationList
eContent	m	The encoded contents DeviationList
certificates	m	States MUST include the Deviation List Signer certificate and SHOULD include the CSCA certificate, which can be used to verify the signature in the signerInfos field.
crls	x	
signerInfos	m	It is RECOMMENDED that States provide only 1 signerinfo within this field.
SignerInfo	m	
version	m	The value of this field is dictated by the sid field. See [RFC 3852]

Value		*Comments*
		Section 5.3 for rules regarding this field
sid	m	
subjectKeyIdentifier	r	It is RECOMMENDED that States support this field over issuerandSerialNumber.
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing States may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving States except to verify the signature value. signedAttrs MUST include signing time (ref. PKCS#9).
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.
signature	m	The result of the signature generation process.
unsignedAttrs	x	

10.2 ASN.1 specification

```
DeviationList
{ joint-iso-itu-t (2) international-organization(23) icao(136) mrtd(1) security(1)
deviationlist(7)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

  -- Imports from RFC 3280 [PROFILE], Appendix A.1
       AlgorithmIdentifier
          FROM PKIX1Explicit88
                 { iso(1) identified-organization(3) dod(6)
                   internet(1) security(5) mechanisms(5) pkix(7)
                   mod(0) pkix1-explicit(18) }

  -- Imports from RFC 3852
       SubjectKeyIdentifier, Digest, IssuerAndSerialNumber
          FROM CryptographicMessageSyntax2004
                 { iso(1) member-body(2) us(840) rsadsi(113549)
                   pkcs(1) pkcs-9(9) smime(16) modules(0)
                   cms-2004(24) };
```

```
DeviationListVersion ::= INTEGER {v0(0)}

DeviationList ::= SEQUENCE {
 version      DeviationListVersion,
 digestAlgorithm AlgorithmIdentifier OPTIONAL,
 deviations   SET OF Deviation
}

Deviation ::= SEQUENCE{
 documents       DeviationDocuments,
 descriptions SET OF DeviationDescription
}

DeviationDescription ::= SEQUENCE{
 description     PrintableString OPTIONAL,
 deviationType   OBJECT IDENTIFIER,
 parameters   [0] ANY DEFINED BY deviationType OPTIONAL,
 nationalUse     [1] ANY OPTIONAL

 -- The nationalUse field is for internal State use, and is not governed
 -- by an ICAO specification.
}

DeviationDocuments ::= SEQUENCE {
 documentType    [0] PrintableString (SIZE(2)) OPTIONAL,
          -- per MRZ, e.g. 'P'
 dscIdentifier   DocumentSignerIdentifier OPTIONAL,
 issuingDate     [4] IssuancePeriod OPTIONAL,
 documentNumbers    [5] SET OF PrintableString OPTIONAL
}

DocumentSignerIdentifier ::= CHOICE{
 issuerAndSerialNumber [1] IssuerAndSerialNumber,
 subjectKeyIdentifier [2] SubjectKeyIdentifier,
 certificateDigest  [3] Digest   --  if  used,  digestAlgorithm  must  be  present  in
DeviationList
}

IssuancePeriod ::= SEQUENCE {
 firstIssued   GeneralizedTime,
 lastIssued   GeneralizedTime
}

-- CertField is used to define which part of a certificate is
  affected by a coding error. Parts of the Body are identified by
  the corresponding value of CertificateBodyField, extensions
  by the corresponding OID identifying the extension.

CertField ::= CHOICE {
 body  CertificateBodyField,
 extension OBJECT IDENTIFIER
```

```
}
CertificateBodyField ::= INTEGER {
 generic(0), version(1), serialNumber(2), signature(3), issuer(4),
 validity(5), subject(6), subjectPublicKeyInfo(7),
 issuerUniqueID(8), subjectUniqueID(9)
}

Datagroup ::= INTEGER
              {dg1(1), dg2(2), dg3(3), dg4(4), dg5(5), dg6(6),
               dg7(7), dg8(8), dg9(9), dg10(10), dg11(11),
               dg12(12), dg13(13), dg14(14), dg15(15), dg16(16),
               sod(20), com(21)}

MRZField ::= INTEGER
              {generic(0), documentCode(1), issuingState(2), personName(3),
               documentNumber(4), nationality(5), dateOfBirth(6),
               sex(7), dateOfExpiry(8), optionalData(9)}

-- Base Object Identifiers

id-icao OBJECT IDENTIFIER ::= {2 23 136 }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 8}

-- Deviation Object Identifiers and Parameter Definitions

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}
id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 1}
id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 2}
id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 3}
id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 4}
id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}
id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}
id-Deviation-LDS-DGHashWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 2}
id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}
id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}
id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}
id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}

END
```

11. REFERENCES (NORMATIVE)

FIPS 180-2	FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, *Secure Hash Standard*, August 2002.
FIPS 186-4	FIPS 186-4, Federal Information Processing Standards Publication (FIPS PUB) 186-4, *Digital Signature Standard (DSS)*, July 2013 (Supersedes FIPS PUB 186-3 dated June 2009).
ISO 3166-1	ISO/IEC 3166-1: 2006, Codes for the representation of names of countries and their subdivisions — Part 1: Country Codes.
ISO/IEC 15946	ISO/IEC 15946: 2002, Information technology — Security techniques — Cryptographic techniques based on elliptic curves.
RFC 3280	RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.
RFC 4055	RFC 4055, J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, June 2005.
RFC 5652	RFC 5652, R. Housley, Cryptographic Message Syntax, September 2009.
RFC 5280	RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May, 2008.
TR 03111	BSI TR-03111: Elliptic Curve Cryptography v 2.0, 2012.
X9.62	X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 7 January 1999.
X.509	ITU-T X.509 | ISO/IEC 9594-8, 2008: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
X.690	ITU-T X.690 2008: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
RFC-RSA	Jonsson, Jakob and Kaliski, Burt RFC 3447, Public-key cryptography standards (PKCS)#1: RSA cryptography specifications version 2.1, 2003
PKCS#1	RSA Laboratories RSA Laboratories Technical Note, PKCS#1 v2.1: RSA cryptography standard, 2002
TLSAES	Chown, P., „Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)“, RFC 3268, June 2002
TLSECC	Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, „Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)“, RFC 4492, May 2006
TLS1.2	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2",

	RFC 5246, August 2008
TLSEXT	Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, „Transport Layer Security (TLS) Extensions“, RFC 4366, April 2006
SOAP	SOAP Version 1.2 Part 1: Messaging framework (Second Edition), W3C Recommendation 27 April 2007
HTTPS	E. Rescorla., „HTTP Over TLS.“, RFC 2818, May 2000
WSI-BP	WS-I Basic Profile available at http://www.ws-i.org/Profiles/BasicProfile-1.1.html
WSI-SSBP	WS-I Basic Binding available at http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html

— — — — — — — —

APPENDIX A TO PART 12 LIFETIMES (INFORMATIVE)

The following examples illustrate calculation of private key usage periods and public key certificate validity for various scenarios as described in Section 4.

A.1 EXAMPLE 1

The first example illustrates a scenario where eMRTDs are valid for five years. Because a relatively large number of eMRTDs are issued per day, the policy is to keep private key usage periods and public key certificate validity to a minimum. For this example, the minimum private key usage period for Document Signer certificates is one month.

Item	***Usage/Validity Period***
eMRTD validity	5 years
Document Signer private key usage period	1 month
Document Signer certificate validity	5 years + 1 month
CSCA private key usage period	3 years
CSCA certificate validity	8 years + 1 month

The consequences of this example are that by the time the first CSCA certificate becomes invalid at least 36 Document Signer certificates will have been issued (one corresponding to each private key that has a one-month usage period). In the last few months before the first CSCA certificate becomes invalid, there will be at least two additional CSCA certificates issued (one corresponding to each private key that has a three-year usage period).

A.2 EXAMPLE 2

The second example illustrates a scenario where eMRTDs are valid for ten years. The policy is to keep private key usage periods and public key certificate validity to an average length.

Item	***Usage/Validity Period***
eMRTD validity	10 years
Document Signer private key usage period	2 months
Document Signer certificate validity	10 years + 2 months
CSCA private key usage period	4 years
CSCA certificate validity	14 years + 2 months

The consequences of this example are by the time the first CSCA certificate becomes invalid at least 24 Document Signer certificates will have been issued (one corresponding to each private key that has a two-month usage period). In the last few months before the first CSCA certificate becomes invalid, there will be at least three additional CSCA certificates issued (one corresponding to each private key that has a four-year usage period).

A.3 EXAMPLE 3

The final example illustrates a scenario where eMRTDs are valid for ten years, and the policy is to use the maximum private key usage periods and public key certificate validity.

Item	***Usage/Validity Period***
eMRTD validity	10 years
Document Signer private key usage period	3 months
Document Signer certificate validity	10 years + 3 months
CSCA private key usage period	5 years
CSCA certificate validity	15 years + 3 months

The consequences of this example are by the time the first CSCA certificate becomes invalid at least 20 Document Signer certificates will have been issued (one corresponding to each private key that has a three-month usage period). In the last few months before the first CSCA certificate becomes invalid, there will be at least three additional CSCA certificates issued (one corresponding to each private key that has a five-year usage period).

— — — — — — — —

APPENDIX B TO PART 12 CERTIFICATE AND CRL PROFILE REFERENCE TEXT (INFORMATIVE)

The certificate and CRL profiles defined in Section 7 are based on definitions and base profile requirements specified in referenced documents. Brief excerpts of some relevant sections from these source documents (as of the time of writing) are replicated in the tables below. These excerpts are provided to assist the reader in understanding the background for some of the requirements specified in the eMRTD certificate and CRL profiles. They are not intended to be relied on instead of the referenced documents. In all cases, to obtain the full specification of the referenced component/extension and to obtain the most current specification, the actual referenced documents MUST be used.

Table 19. Certificate Fields and Extensions

Component / Extension	***Reference***	***Relevant Excerpts***
`Certificate`	RFC 5280 – 4.1.1	
`TBSCertificate`	RFC 5280 – 4.1.1.1	
`signatureAlgorithm`	RFC 5280 – 4.1.1.2	
`signatureValue`	RFC 5280 – 4.1.1.3	
`TBSCertificate`	RFC 5280 – 4.1.2	
`version`	RFC 5280 – 4.1.2.1	When extensions are used, as expected in this profile, version MUST be 3 (value is `2`).
`serialNumber`	RFC 5280 – 4.1.2.2	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the `serialNumber` to be a non-negative integer. Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle `serialNumber` values up to 20 octets. Conformant CAs MUST NOT use `serialNumber` values longer than 20 octets.

Component / Extension	*Reference*	*Relevant Excerpts*
	X.690 – 8.3.2	If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero. *Note*. — These rules ensure that an integer value is always encoded in the smallest possible number of octets.
	X.690 – 8.3.3	The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
`signature`	RFC 5280 – 4.1.1.2	This field MUST contain the same algorithm identifier as the `signatureAlgorithm` field in the sequence `Certificate`.
`issuer`	RFC 5280 – Appendix A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))`
	RFC 5280 – 4.1.2.4	CAs conforming to this profile MUST use either the `PrintableString` or `UTF8String` encoding of `DirectoryString`.
	ISO 3166-1	
`validity`	RFC 5280 – 4.1.2.5	Both `notBefore` and `notAfter` may be encoded as `UTCTime` or `GeneralizedTime`. CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as `UTCTime`. Certificate validity dates in 2050 or later MUST be encoded as `GeneralizedTime`.
`(if encoded as UTCTime)`	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on `UTCTime`.
	X.690 – 11.8.2	The seconds element shall always be present.
`(if encoded as GeneralizedTime)`	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on `GeneralizedTime`.
	X.690 – 11.7.2	The seconds element shall always be present.

Component / Extension	***Reference***	***Relevant Excerpts***
	RFC 5280 – 4.1.2.5.2	`GeneralizedTime` values MUST NOT include fractional seconds. For the purposes of this profile, `GeneralizedTime` values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
`subject`	RFC 5280 – Appendix A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))`
	RFC 5280 – 4.1.2.6	CAs conforming to this profile MUST use either the `PrintableString` or `UTF8String` encoding of `DirectoryString`.
`subjectPublicKeyInfo`	RFC 5280 – 4.1.2.7	
`issuerUniqueID`	RFC 5280 – 4.1.2.8	CAs conforming to this profile MUST NOT generate certificates with unique identifiers.
`subjectUniqueID`	RFC 5280 – 4.1.2.8	CAs conforming to this profile MUST NOT generate certificates with unique identifiers.
`extensions`	X.690 – 11.5	The encoding of a `set` value or `sequence` value shall not include an encoding for any component value which is equal to its default value.
`AuthorityKeyIdentifier`	RFC 5280 – 4.2.1.1	The `keyIdentifier` field of the `authorityKeyIdentifier` extension MUST be included in all certificates generated by conforming CAs to facilitate certification path construction. There is one exception. Where a CA distributes its public key in the form of a “self-signed” certificate, the authority key identifier MAY be omitted.
`keyIdentifier`		
`authorityCertIssuer`		
`authorityCertSerialNumber`		

Component / Extension	*Reference*	*Relevant Excerpts*
SubjectKeyIdentifier	RFC 5280 – 4.2.1.2	To facilitate certification path construction, this extension MUST appear in all conforming CA certificates, that is, all certificates including the basic constraints extension (section 4.2.1.9) where the value of cA is TRUE.
subjectKeyIdentifier		
KeyUsage	RFC 5280 – 4.2.1.3	The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.
digitalSignature		The digitalSignature bit is asserted when the subject public key is used with a digital signature mechanism to support security services other than certificate signing (bit 5), or CRL signing (bit 6).
nonRepudiation		
keyEncipherment		
dataEncipherment		
keyAgreement		
keyCertSign		The keyCertSign bit is asserted when the subject public key is used for verifying a signature on public key certificates.
cRLSign		The cRLSign bit is asserted when the subject public key is used for verifying a signature on certificate revocation list (e.g., a CRL, delta CRL, or an ARL). This bit MUST be asserted in certificates that are used to verify signatures on CRLs.
encipherOnly		
decipherOnly		
PrivateKeyUsagePeriod	RFC 3280 – 4.2.1.4	CAs conforming to this profile MUST NOT generate certificates with private key usage period extensions unless at least one of the two components is present and the extension is non-critical.
notBefore		Where used, notBefore and notAfter are represented as GeneralizedTime and MUST be specified and interpreted as defined in section 4.1.2.5.2.
notAfter		

Component / Extension	***Reference***	***Relevant Excerpts***
`CertificatePolicies`	RFC 5280 – 4.2.1.4	If this extension is critical, the path validation software MUST be able to interpret this extension (including the optional qualifier), or MUST reject the certificate.
`PolicyInformation`		
`policyIdentifier`		
`policyQualifiers`		
`PolicyMappings`	RFC 5280 – 4.2.1.5	
`SubjectAltName`	RFC 5280 – 4.2.1.6	
`IssuerAltName`	RFC 5280 – 4.2.1.7	
`SubjectDirectoryAttributes`	RFC 5280 – 4.2.1.8	
`Basic Constraints`	RFC 5280 – 4.2.1.9	The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. Conforming CAs MUST include this extension in all CA certificates that contain public keys used to validate digital signatures on certificates and MUST mark the extension as critical in such certificates.
`cA`		The `cA` boolean indicates whether the certified public key belongs to a CA. If the `cA` boolean is not asserted, then the `keyCertSign` bit in the key usage extension MUST NOT be asserted.
`PathLenConstraint`		
`NameConstraints`	RFC 5280 – 4.2.1.10	
`PolicyConstraints`	RFC 5280 – 4.2.1.11	
`ExtKeyUsage`	RFC 5280 – 4.2.1.12	This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.

Component / Extension	*Reference*	*Relevant Excerpts*
CRLDistributionPoints	RFC 5280 – 4.2.1.13	
distributionPoint		
reasons		
cRLIssuer		
InhibitAnyPolicy	RFC 5280 – 4.2.1.14	
FreshestCRL	RFC 5280 – 4.2.1.15	
privateInternetExtensions	RFC 5280 – 4.2.2	
NameChange		
DocumentType		
Netscape Certificate Type		
other private extensions		

Table 20. CRL Fields and Extensions

Component / Extension	*Reference*	*Relevant Excerpts*
CertificateList	RFC 5280 – 5.1.1	
tBSCertList	RFC 5280 – 5.1.1.1	
signatureAlgorithm	RFC 5280 – 5.1.1.2	
signatureValue	RFC 5280 – 5.1.1.3	
	RFC 5280 – 5.1.2	
version	RFC 5280 – 5.1.2.1	This optional field describes the version of the encoded CRL. When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is 1).
signature	RFC 5280 – 5.1.2.2	This field MUST contain the same algorithm identifier as the signature field in the sequence CertificateList.

Component / Extension	***Reference***	***Relevant Excerpts***
issuer	RFC 5280 – Appendix A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE 1..ub-serial-number))`
	RFC 5280 – 5.1.2.3 and 4.1.2.4	CAs conforming to this profile MUST use either the `PrintableString` or `UTF8String` encoding of `DirectoryString`.
thisUpdate	RFC 5280 – 5.1.2.4	CRL issuers conforming to this profile MUST encode `thisUpdate` as `UTCTime` for dates through the year 2049. CRL issuers conforming to this profile MUST encode `thisUpdate` as `GeneralizedTime` for dates in the year 2050 or later.
(if encoded as UTCTime)	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on `UTCTime`.
	X.690 – 11.8.2	The seconds element shall always be present.
(if encoded as GeneralizedTime)	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on `GeneralizedTime`.
	X.690 – 11.7.2	The seconds element shall always be present.
	RFC 5280 – 4.1.2.5.2	`GeneralizedTime` values MUST NOT include fractional seconds. For the purposes of this profile, `GeneralizedTime` values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
nextUpdate	5.1.2.5	CRL issuers conforming to this profile MUST encode `nextUpdate` as `UTCTime` for dates through the year 2049. CRL issuers conforming to this profile MUST encode `nextUpdate` as `GeneralizedTime` for dates in the year 2050 or later.
(if encoded at UTCTime)	X.690 – 11.8.1	The encoding shall terminate with "Z", as described in the ITU-T X.680 | ISO/IEC 8824-1 clause on `UTCTime`.
	X.690 – 11.8.2	The seconds element shall always be present.
(if encoded at GeneralizedTime)	X.690 – 11.7.1	The encoding shall terminate with a "Z", as described in the ITU-T Rec. X.680 | ISO/IEC 8824-1 clause on `GeneralizedTime`.
	X.690 – 11.7.2	The seconds element shall always be present.

Component / Extension	*Reference*	*Relevant Excerpts*
	RFC 5280 – 4.1.2.5.2	`GeneralizedTime` values MUST NOT include fractional seconds. For the purposes of this profile, `GeneralizedTime` values MUST be expressed Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero.
`revokedCertificates`	RFC 5280 – 5.1.2.6	When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers.
`crlExtensions`	RFC 5280 – 5.2	Conforming CRL issuers are REQUIRED to include the authority key identifier (Section 5.2.1) and the CRL number (Section 5.2.3) extensions in all CRLs issued.
	X.690 – 11.5	The encoding of a `set` value or `sequence` value shall not include an encoding for any component value which is equal to its default value.
`authorityKeyIdentifier`	RFC 5280 – 5.2.1	Conforming CRL issuers MUST use the key identifier method, and MUST include this extension in all CRLs issued.
`issuerAlternativeName`	RFC 5280 – 5.2.2	
`cRLNumber`	RFC 5280 – 5.2.3	CRL issuers conforming to this profile MUST include this extension in all CRLs and MUST mark this extension as non-critical. `CRLNumber ::= INTEGER (0..MAX)` Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle `CRLNumber` values up to 20 octets. Conforming CRL issuers MUST NOT use `CRLNumber` values longer than 20 octets.
	X.690 – 8.3.2	If the contents octets of an integer value encoding consist of more than one octet, then the bits of the first octet and bit 8 of the second octet: a) shall not all be ones; and b) shall not all be zero. *Note*.— These rules ensure that an integer value is always encoded in the smallest possible number of octets.

Component / Extension	***Reference***	***Relevant Excerpts***
	X.690 – 8.3.3	The contents octets shall be a two's complement binary number equal to the integer value, and consisting of bits 8 to 1 of the first octet, followed by bits 8 to 1 of the second octet, followed by bits 8 to 1 of each octet in turn up to and including the last octet of the contents octets.
`deltaCRLIndicator`	RFC 5280 – 5.2.4	
`issuingDistributionPoint`	RFC 5280 – 5.2.5	
`freshestCRL`	RFC 5280 – 5.2.6	
`reasonCode`	RFC 5280 – 5.3.1	
`holdInstructionCode`	RFC 5280 – 5.3.2	
`invalidityDate`	RFC 5280 – 5.3.3	
`certificateIssuer`	RFC 5280 – 5.3.4	

— — — — — — — —

APPENDIX C TO PART 12 EARLIER CERTIFICATE PROFILES (INFORMATIVE)

The certificate profiles in this Appendix were specified in the Sixth Edition of ICAO Doc 9303. Although CSCAs MUST issue certificates that comply with the current profiles as specified in Section 7, the earlier profiles are included here for information only as certificates that were issued in compliance with the earlier profiles will be in circulation, and processed by Inspection Systems for several years.

Table 21. Certificate Body

Certificate Component	***Section in RFC 3280***	***Country Signing CA Certificate***	***Document Signer Certificate***	***Comments***
`Certificate`	4.1.1	m	m	
`TBSCertificate`	4.1.1.1	m	m	See next part of the table
`SignatureAlgorithm`	4.1.1.2	m	m	Value inserted here dependent on algorithm selected
`SignatureValue`	4.1.1.3	m	m	Value inserted here dependent on algorithm selected
`TBSCertificate`	4.1.2			
`version`	4.1.2.1	m	m	SHALL be `v3`
`serialNumber`	4.1.2.2	m	m	
`signature`	4.1.2.3	m	m	Value inserted here SHALL match the OID in `signatureAlgorithm`
`issuer`	4.1.2.4	m	m	
`validity`	4.1.2.5	m	m	Implementations SHALL specify using UTC time until 2049 from then on using `GeneralizedTime`
`subject`	4.1.2.6	m	m	
`subjectPublicKeyInfo`	4.1.2.7	m	m	
`issuerUniqueID`	4.1.2.8	x	x	
`subjectUniqueID`	4.1.2.8	x	x	

Certificate Component	*Section in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
extensions	4.1.2.9	m	m	See next table on which extensions SHOULD be present

Table 22. Extensions

Extension name	*Paragraph in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
AuthorityKeyIdentifier	4.2.1.1	o	m	Mandatory in all certificates except for self-signed CSCA certificates
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	This extension SHALL be marked CRITICAL
PrivateKeyUsagePeriod	4.2.1.4	o	o	This would be the issuing period of the private key
CertificatePolicies	4.2.1.5	o	o	
PolicyMappings	4.2.1.6	x	x	
SubjectAltName	4.2.1.7	x	x	
IssuerAltName	4.2.1.8	x	x	
SubjectDirectoryAttributes	4.2.1.9	x	x	
BasicConstraints	4.2.1.10	mc	x	This extension SHALL be marked CRITICAL
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	

Extension name	*Paragraph in RFC 3280*	*Country Signing CA Certificate*	*Document Signer Certificate*	*Comments*
CRLDistributionPoints	4.2.1.14	o	o	If issuing States or organizations choose to use this extension they SHALL include the ICAO PKD as a distribution point. Implementations may also include relative CRL DPs for local purposes; these may be ignored by other receiving States.
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	N/A	o	o	If any private extension is included for national purposes then it SHALL NOT be marked. Issuing States or organizations are discouraged from including any private extensions.
AuthorityKeyIdentifier	4.2.1.1			
keyIdentifier		m	m	If this extension is used this field SHALL be supported as a minimum
authorityCertIssuer		o	o	
authorityCertSerialNumber		o	o	
SubjectKeyIdentifier	4.2.1.2			
subjectKeyIdentifier		m	m	
KeyUsage	4.2.1.3			
digitalSignature		x	m	
nonRepudiation		x	x	
keyEncipherment		x	x	
dataEncipherment		x	x	
keyAgreement		x	x	
keyCertSign		m	x	

Extension name	***Paragraph in RFC 3280***	***Country Signing CA Certificate***	***Document Signer Certificate***	***Comments***
cRLSign		m	x	
encipherOnly		x	x	
decipherOnly		x	x	
BasicConstraints	4.2.1.10			
cA		m	x	TRUE for CA certificates
PathLenConstraint		m	x	0 for New CSCA certificate, 1 for Linked CSCA certificate
CRLDistributionPoints	4.2.1.14			
distributionPoint		m	x	
reasons		m	x	
cRLIssuer		m	x	
CertificatePolicies	4.2.1.5			
PolicyInformation				
policyIdentifier		m	m	
policyQualifiers		o	o	

— — — — — — — —

APPENDIX D TO PART 12 RFC 5280 VALIDATION COMPATIBILITY (INFORMATIVE)

This Appendix provides guidance to receiving States wishing to use systems that implement the [RFC 5280] certification path and CRL validation algorithms.

The eMRTD PKI trust model is a subset of that covered by the validation procedures defined in [RFC 5280]. Section D.1 identifies the subset of steps from the [RFC 5280] definition that are required for the eMRTD application and provides the necessary inputs and initialization values and processes for certification path validation, CRL validation and revocation checking.

Section D.2 covers the remaining steps from the [RFC 5280] definition that are not relevant to the eMRTD application. The inputs and initialization values for certification path validation and CRL validation are provided. The guidance in this section is for use in situations where the tools implement the full [RFC 5280] algorithms, rather than just the subset described in D.1.

Section D.3 provides guidance to support the extension of [RFC 5280] based CRL processing to cover revocation checking after a CSCA has undergone a name change.

D.1 Steps Relevant to eMRTD

The eMRTD certification path validation procedure defined here is based on the procedure described in [RFC 5280].The same terminology and process descriptions are used. The eMRTD certificate profiles restrict certification paths to a single certificate and prohibit use of many optional features that are used in other applications, such as the Internet PKI defined in [RFC 5280]. Path validation steps associated with these features are omitted from the eMRTD certification path validation procedure.

D.1.1 Certification Path Validation Procedure

D.1.1.1 Inputs

[RFC 5280] defines a set of nine inputs to the path validation algorithm. Only the following three are relevant to the eMRTD application:

- certification path: A single certificate (e.g. the Document Signer certificate);
- current date/time; and
- Trust Anchor information, including:
    - trusted issuer name: If the Trust Anchor is in the form of a CSCA certificate, the trusted issuer name is the value of the `subject` field of that certificate;
    - trusted public key algorithm: If the Trust Anchor is in the form of a CSCA certificate, the trusted public key algorithm is taken from the `SubjectPublicKeyInfo` field of that certificate;

- trusted public key: If the Trust Anchor is in the form of a CSCA certificate, the trusted public key is taken from the `SubjectPublicKeyInfo` field of that certificate; and

- trusted public key parameters: This is an optional input that is included only if the trusted public key algorithm requires parameters. If the Trust Anchor is in the form of a CSCA certificate, these parameters are taken from the `SubjectPublicKeyInfo` field of that certificate.

If an implementation requires that the additional six inputs be supplied, recommendations for these are provided in D.2.

There could be several Trust Anchors for the CSCA that issued the certificate being validated. Of these Trust Anchors, the one that MUST be used is the one that contains the public key that matches the value of the Authority Key Identifier extension in the certificate being validated.

D.1.1.2 Initialization

There are eleven State variables defined in [RFC 5280]. Only the following five are relevant to the eMRTD application:

- application: max_path_length: Initialize to “0”;
- working_issuer_name: Initialize to the value of the trusted issuer name;
- working_public_key_algorithm: Initialize to the value of the trusted public key algorithm;
- working_public_key: Initialize to the value of the trusted public key; and
- working_public_key_parameters: Initialize to the value of the trusted public key parameters.

If an implementation requires that the additional six variables be initialized, recommendations for these are provided in D.2.

D.1.1.3 Certificate processing

eMRTD certificate processing steps are a subset of those defined in [RFC 5280]. The result of processing an eMRTD certificate using this simplified process will be consistent with the result using the full RFC 5280 algorithm. If the additional inputs and State variables are configured as described in D.2:

a) Verify the basic certificate information. The certificate MUST satisfy each of the following:

   - the signature on the certificate can be verified using working_public_key_algorithm, the working_public_key, and the working_public_key_parameters;
   - the certificate validity period includes the current time;
   - at the current time, the certificate is not revoked (see 6.3 for details); and
   - the certificate issuer name is the working_issuer_name.

b) Assign the certificate `subjectPublicKey` to working_public_key.

c) If the `subjectPublicKeyInfo` field of the certificate contains an algorithm field with non-null

parameters, assign the parameters to the working_public_key_parameters variable. If the `subjectPublicKeyInfo` field of the certificate contains an algorithm field with null parameters or parameters are omitted, compare the certificate `subjectPublicKey` algorithm to the working_public_key_algorithm. If the certificate `subjectPublicKey` algorithm and the working_public_key_algorithm are different, set the working_public_key_parameters to null.

d) Assign the certificate `subjectPublicKey` algorithm to the working_public_key_algorithm variable.

e) Recognize and process any other critical extensions present in the certificate.

f) Process any other recognized non-critical extensions present in the certificate.

If any of the checks in step a) fail or if there are any unrecognized critical extensions in the certificate that cannot be processed, the path validation procedure fails. Otherwise the procedure succeeds.

D.1.1.4 Outputs

If path validation succeeds, the procedure terminates, returning a success indication together with the working_public_key, the working_public_key_algorithm, and the working_public_key_parameters.

If path validation fails, the procedure terminates, returning a failure indication and an appropriate reason.

D.1.2 CRL Validation and Revocation Checking

The CRL validation algorithm in [REC 5280] covers various types of CRLs including delta CRLs, partitioned CRLs, indirect CRLs, etc. The CRL profile for the eMRTD application is very restrictive and prohibits use of any of these features. Use of the `issuingDistributionPoint` extension as well as all of the standardized CRL-entry extensions is also prohibited. As a result, CRL validation and revocation checking for the eMRTD application is relatively simple.

D.1.2.1 Inputs

[RFC 5280] defines two inputs to the CRL validation algorithm. Only the following one of these is relevant to the eMRTD application. If an implementation requires that the additional input be supplied, a recommendation for this is provided in D.2.

- certificate: certificate serial number and issuer name

D.1.2.2 Initialization

There are three State variables defined in [RFC 5280]. Only the following one of these is relevant to the eMRTD application. If an implementation requires that the additional two variables be initialized, recommendations for these are provided in D.2.

- cert_status : initialize to the value UNREVOKED.

D.1.2.3 CRL Processing

All CRLs in the eMRTD application are complete CRLs that cover all current certificates issued by the CSCA that issued the CRL. There are no partitioned, delta or indirect CRLs. The steps in the CRL processing algorithm for the eMRTD application are:

a) Obtain the current CRL for the CSCA that issued the certificate. If the CRL cannot be obtained, the cert_status variable is set to UNDETERMINED, and processing is stopped.

b) Verify that the CRL issuer is the same CSCA that issued the certificate in question. Because there is a single CSCA in each country, and the eMRTD application is a closed application with Inspection Systems retaining a cache of CRLs that is unique to this application, verifying that the country name is the same in the issuer field of the CRL and the issuer field of the certificate is sufficient.

- If the CSCA has not undergone a name change since the certificate was issued, the issuer field in the CRL and the issuer field in the certificate will be identical.

- If the CSCA has undergone a name change since the certificate was issued, the country attribute of the name in the issuer field of the certificate and in the issuer field of the CRL will be the same, but some other attributes may be different.

- If the relying party wishes to verify that substitution of some non eMRTD CRL has not happened, it may optionally verify that it has Trust Anchors for both CSCA names and that those Trust Anchors are for the same CSCA. If the CSCA has undergone a name change and has included the optional `issuerAltName` extension in the CRL, the relying party MAY optionally verify that the issuer field in the certificate is identical to one of the values in this extension.

If the CRL issuer is not the CSCA that issued the certificate, the cert_status variable is set to UNDETERMINED, and processing is stopped.

c) Validate the certification path for the issuer of the CRL. Note that in the eMRTD application all CRLs are issued by CSCAs that are the Trust Anchors for the respective paths. Unlike the algorithm in [RFC 5280], the eMRTD application does NOT require that the Trust Anchor used to validate the CRL certification path be the same Trust Anchor that was used to validate the target certificate. However, if the Trust Anchors are different, they MUST both be Trust Anchors for the same CSCA. Unlike [RFC 5280], the eMRTD application has multiple Trust Anchors for a given CSCA that are valid at the same time. If the certification path cannot be successfully validated, the cert_status variable is set to UNDETERMINED, and processing is stopped.

d) Verify the signature on the CRL. If the signature cannot be successfully verified, the cert_status variable is set to UNDETERMINED, and processing is stopped.

e) Search for the certificate on the CRL. If an entry is found that matches the certificate issuer and serial number, then the cert_status variable is set to UNSPECIFIED.

D.1.2.4 Output

Return the cert_status. If steps a), b), c) or d) failed, the status will be UNDETERMINED. If the certificate was listed as revoked on the CRL, the status will be UNSPECIFIED. If CRL validation succeeded, but the certificate was not listed on the CRL, the status will be UNREVOKED.

D.2 Steps not Required by eMRTD

D.2.1 Certification Path Validation

Settings for additional inputs that are not relevant to eMRTD validation include:

- initial-policy-mapping-inhibit: Set to inhibit policy mapping;
- initial-any-policy-inhibit: Set to inhibit processing of the any-policy value;
- initial-permitted-subtrees: Set to permit all subtrees;
- initial-excluded-subtrees: Set to exclude no subtrees;
- initial-explicit-policy: This should NOT be set; and
- user-initial-policy-set: Set to the special value “any-policy”.

Initialization of State variables that are not relevant to the eMRTD application include:

- permitted_subtrees: Initialize to permit all subtrees;
- excluded_subtrees: Initialize to exclude no subtrees;
- inhibit_any_policy: If initial-any-policy-inhibit is set, initialize to “0”. Otherwise, set to the value 1 or any value greater than that;
- policy_mapping: Initialize to “0”;
- explicit_policy: Initialize to “2”; and
- valid_policy_tree: Initialize the valid_policy element to “anyPolicy”, the qualifier_set element to empty and the expected_policy_set to “anyPolicy”.

D.2.2 CRL Validation

Settings for additional inputs that are not relevant to eMRTD validation include:

- use-deltas: Set to prohibit use of deltas.

Initialization of State variables that are not relevant to the eMRTD application include:

- reasons_mask: Initialize to an empty set; and
- Interim_reasons_mask: Initialize to the special value “all-reasons”.

D.3 Modifications required to process CRLs

CRL validation systems that comply with the CRL validation procedure in [RFC 5280] are not intended to support environments where a CA has undergone a name change, such as the eMRTD application environment. Therefore these systems require some modification to handle this special case, as described below:

a) In clause 6.3.3, step a) of the [RFC 5280] CRL validation procedure, the name in the distribution point field of the CRL Distribution Points extension of the certificate in question is used to update the local cache with the relevant CRL(s). For the eMRTD application, this step would need to be modified and only the `countryName` attribute of the distribution point field should be used to identify and obtain the appropriate CRL.

b) In clause 6.3.3, step f) of the [RFC 5280] CRL validation procedure, there is a requirement that the same Trust Anchor be used to validate the certification path for the CRL issuer that was used to validate the target certificate. This is NOT a requirement for the eMRTD application because independent Trust Anchors are established for each public key of the CSCA.

The Trust Anchor used for validation of the CRL issuer will be the one for the CSCA's public key that corresponds to the private key used to sign the CRL. The Trust Anchor used to validate the certification path for the target certificate may be for an earlier CSCA key pair.

APPENDIX E TO PART 12 LDS2 EXAMPLE (INFORMATIVE)

The following example illustrates the interactions between the different components of the LDS2 Signature PKI and the LDS2 Authorization PKI.

To illustrate the interactions and preliminaries required for a typical business scenario, consider the scenario where the country of Dystopia wants to write travel stamps to passports of citizens of the country of Utopia. Later, the country of Atlantis wants to read travels stamps written by Dystopia on Utopia's passports.

Preliminaries:

- Utopia has installed an LDS 2 Travel Stamp application on their passports.
- Both Dystopia and Utopia have set up their LDS2 Authorization PKI.
- Dystopia has set up their LDS1 Signing PKI to issue LDS2 Signer Certificates.
- CVCA certificates and SPOC client and server certificates were exchanged in a trusted manner between Utopia and Dystopia at some point in time (subsequently, new CVCA and SPOC certificates can be exchanged directly via the SPOC).
- CVCA certificates and SPOC client and server certificates were exchanged in a trusted manner between Utopia and Atlantis at some point in time (subsequently, new CVCA and SPOC certificates can be exchanged directly via the SPOC). If the LDS2 travel stamp application is open for reading, i.e. any country can read LDS2 travel stamps (permission is only needed for writing), this step can be omitted.
- CSCA certificates have been exchanged in a trusted manner between Dystopia and Atlantis at some point in time.

Recurring process in order to enable Dystopia to electronically stamp Utopia's eMRTDs:

- Dystopia requests a DV certificate from Utopia.
- Dystopia's SPOC uses its SPOC client certificate and Utopia's SPOC server certificate to initiate a SPOC connection. Then a request is generated by a dystopian DV, and sent from SPOC to SPOC. Upon request, Utopia generates a foreign DV certificate with read/write access for Dystopia, and the certificate is delivered back via SPOC to SPOC.
- Upon receiving the DV certificate from its SPOC, the DV of Dystopia generates Terminal Certificates for the terminals of its borders. Connecting to the passport, the IC on the utopian passports verifies the terminal certificate of Dystopia with the DV certificate of Dystopia, and the DV certificate of Dystopia with the CVCA certificate of Utopia. The IC then grants read/write access for the dystopian terminal to the LDS2 Travel Stamp application.

Process to electronically stamp an eMRTD:

- Dystopia creates an electronic travel stamp, and signs it with the private key corresponding to the public key stored in an LDS2 (Travel Stamp) Signer certificate of the LDS2 Signing PKI of Dystopia. The LDS2 Signer certificate is stored on the contactless IC of the utopian passport.

Upon encountering the utopian passport at the border of Atlantis:

- If reading travel stamps from utopian passports requires a terminal certificate with read-access, a certificate request from Atlantis is sent via SPOC-to-SPOC to Utopia. Upon request, Utopia generates a foreign DV certificate with read-access for Atlantis and sends this certificate to Atlantis via SPOC-to-SPOC. Using that DV certificate, Atlantis generates terminal certificates with read-access for utopian passports for Atlantis' terminals. I travel stamps in utopian passports can be read by any terminal, this

step can be omitted.

- To verify a travel stamp of the passport written by Dystopia, Atlantis uses the LDS1 signing PKI of Dystopia: The dystopian LDS2 Signer certificate stored in the passport is used to verify the travel stamp. Then the chain is build up, i.e. the Dystopia LDS2 Signer certificate is verified with the Dystopia CSCA certificate received preliminarily.

— END —

ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2020

Part 13: Visible Digital Seals

Approved by the Secretary General and published under his authority

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/Security/FAL/TRIP

Doc 9303, *Machine Readable Travel Documents*
Part 13 — *Visible Digital Seals*
ISBN 978-92-9249-799-6

DOCUMENT CHANGE RECORD

Doc 9303, Part 13

DATE	NO.	SECTION/PAGES AFFECTED

TABLE OF CONTENTS

1. SCOPE

This Part 13 of Doc 9303 specifies a digital seal to ensure the authenticity and integrity of non-electronic documents in a comparatively cheap, but highly secure manner using asymmetric cryptography. The information on the non-electronic document is cryptographically signed, and the signature is encoded as a two-dimensional bar code and printed on the document itself. This approach – the *visible digital seal* – provides the following advantages:

- *Asymmetry*. Due to using asymmetric cryptography, the cost of attacking a digital seal is considerably higher than the cost of issuing a document protected with a digital seal. Thus even though the cost of issuing a document is very low, it is extremely costly to fake or forge the personalisation data of that document.
- *Personalization*. Each digital seal verifies the information printed on the physical document, and is thus tied to the document holder. There is no direct equivalent of a blank document, and thus no blanks can be lost or stolen.
- *Easy verification*. Even untrained persons are able to verify a document protected with a digital seal by using low cost equipment, such as an application on a smartphone. Moreover, due to the binary nature of a digital signature, distinguishing between authentic and forged documents is easy.

While the digital seal provides a considerable security improvement for (usually paper-based) documents having no microchip, it has considerable limitations when compared to chip-based documents. Storage capacity of digital seals is usually limited to a few kByte at most and neither the data nor the cryptographic keys or schemes for the digital seal can be updated on existing documents. That is, cryptographic agility is not supported. The digital seal does not provide any protection against cloning, does not implement privacy protection functionality, and is more prone to read errors due to wear and tear than chip based documents. Besides, the versatility of crypto chips allows implementation of additional features like signature schemes, terminal authentication, two factor authentication methods based on shared secrets like a PIN, or secure cryptographic protocols based on symmetric schemes. As 2D bar codes can by no means replace the functional or security features of microchips, travel documents shall employ microchips whenever feasible.

2. DIGITAL SEAL ENCODING

A visible digital seal is a cryptographically signed data structure containing document features, encoded as a 2D bar code and printed on a document. This section gives a definition of the encoding and structure of a visible digital seal.

2.1 Bar code Format and Print Requirements

This specification defines how data are encoded into a stream of bytes. Only 2D bar codes whose symbology is specified as an ISO standard SHALL be used. ISO standardized 2D bar codes symbologies include for example DataMatrix [ISO/IEC 16022], Aztec Codes [ISO/IEC 24778], and QR Codes [ISO/IEC 18004].

The bar code SHOULD be printed in a way, that allows reader equipment (i.e. off-the-shelf smartphones or scanners) to reliably decode the bar code; in particular [ISO/IEC 15415] SHOULD be taken into account when assessing print quality. The resulting printing and scanning quality requirements depend on the document and application scenario specific details MAY be specified in a profile. Due to the fact that the quality of printing and scanning affects error rates and influences the robustness of digital seal verification, these requirements SHOULD ensure that the bar code containing the digital seal and all mandatory document features can be reliably verified. Another important requirement addresses symbol contrast of the bar code, because the digital seal might be printed on security paper with a colored background (e.g. green).

When using standard inkjet printers, it is RECOMMENDED to print with a module size (size of one block of a 2D bar code) of at least 0.3386mm sidelength per module, corresponding to 4 dots per module sidelength (i.e. 16 dots per module) on a 300dpi printer, or 8 dots per module sidelength (i.e. 64 dots per module) on a 600 dpi printer. Smaller printing sizes MAY be acceptable, if high-resolution printers or laser-printers are used. For the placement of the bar code on the document see the respective parts of Doc 9303.

The encoded bar code consists of a header (see Section 2.2), message (see Section 2.3), and signature zone (see Section 2.4). An overview of the structure is given in Figure 1.

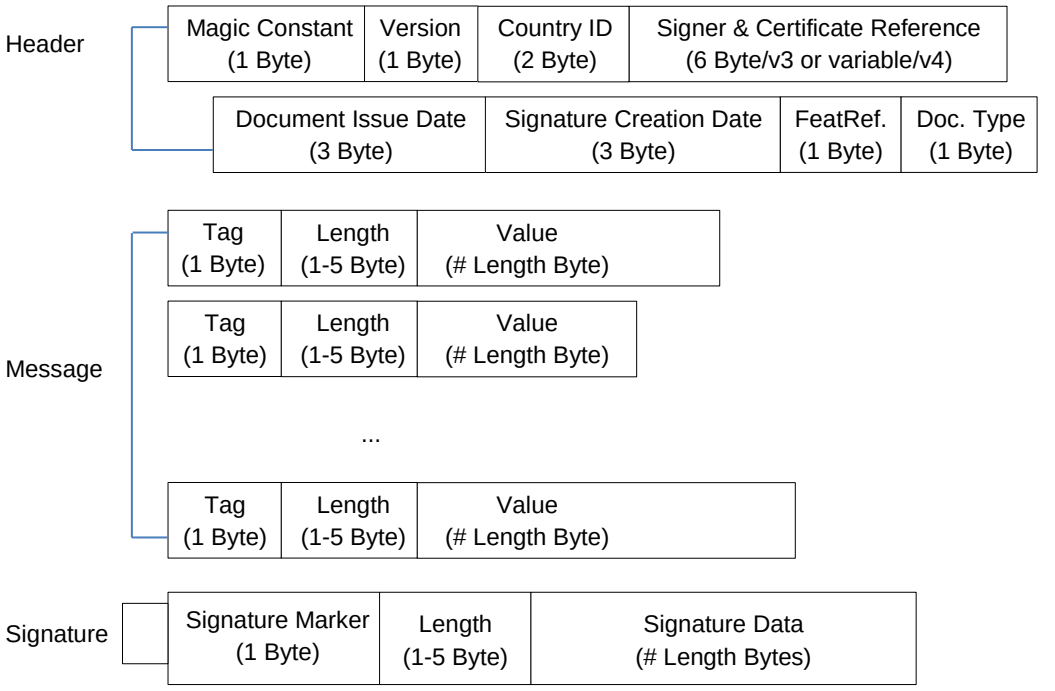


Figure 1. Digital Seal Structure

2.2 Header

The header contains meta-data about the document and the encoding, such as a version number, and document issuance and signature creation dates.

This specification defines two versions of the header, denoted by Version Identifier “3” and “4”, respectively. The versions differ in the definition of the certificate reference (see below) and the length encoding of document features (see Section 2.3)

The overall length of the header is 18 bytes for version 3 and variable for version 4. A definition of the header is given in Table 1.

Table 1: Format of the Header

Start Position	Length (Byte)	Content
0x00	1	*Magic Constant*. The magic constant has a fixed value of 0xDC identifying a bar code conforming to this specification.
0x01	1	*Version*. A byte value identifying the version of this specification. The versions defined in this specification are identified by the byte value 0x02 / 0x03, respectively. The number n indicates version n+1, e.g. a value 0 indicates version 1.
0x02	2	*Issuing Country*. A three letter code identifying the issuing state or organization. The three letter code is according to Doc 9303-3. If the three letter code comprises less than three letters, the code MUST be padded with filler characters (‘<’), e.g. ‘D’ is padded to ‘D<<’. The code is encoded by C40 (cf. Section 2.6) as a two-byte sequence.
0x04	6 / v	*Signer Identifier and Certificate Reference*. Version 3: A nine letter code identifying the (bar code) Signer and the certificate. Version 4: A variable length letter code identifying the (bar code) Signer and the certificate (‘v’ denotes the overall length of this field). The code is encoded by C40 (cf. Section 2.6). For variable length encoding see Section 2.2.1.
0x0A / 0x04+v	3	*Document Issue Date*. The date the document was issued. Encoded as defined in Section 2.3.1.
0x0D / 0x07+v	3	*Signature Creation Date*. The date the signature was created. Encoded as defined in Section 2.3.1.
0x10 / 0x0A+v	1	*Document Feature Definition Reference*. A reference code to a document that defines the number and encoding of document features. This definition is independent for each document type category, i.e. the same document feature definition reference code may have different meanings for different document type categories. Values MUST be in the range between 01dec and 254dec.
0x11 / 0x0B+v	1	*Document Type Category*. The category of the document, e.g. (visa, emergency travel document, birth certificate, etc.). Odd numbers in the range between 01dec and 253dec SHALL be used for ICAO specified Document Type Categories.

Sum	18 / 12 + v

2.2.1 Signer Identifier and Certificate Reference

Due to size restrictions, it is impossible to store the certificates that contain the public key corresponding to the signature within the bar code. Therefore, the certificate MUST be acquired on a different channel. In order to uniquely identify the certificate and the signer that is the subject of the certificate, and to link the certificate to the bar code, a string containing the signer identifier and a reference to the certificate is stored in the header. This string consists of:

1. The *Signer Identifier*: The combination of the two letter country code according to Doc 9303-3 of the Signer's country and of two alphanumeric characters to identify a Signer within the above defined country. The Signer Identifier MUST be unique for a Signer in a given country.

2. The *Certificate Reference*:

    a. For header version 3: A hex-string of exactly five characters that MUST uniquely identify a certificate for a given Signer.

    b. For header version 4: A hex-string comprising the concatenation of

        i. exactly two characters denoting the number of following characters, and

        ii. characters that MUST uniquely identify a certificate for a given Signer.

Note that for the specific use case of visas (cf. Doc 9303-7) the Signer is the *Visa Signer*.

The Certificate Reference `0 ... 0` is reserved for testing purposes and MUST NOT be used in production.

The (bar code) Signer Identifier and Certificate Reference MUST correspond to the Subject Distinguished Name (DN) and the serial number, respectively, of a Signer Certificate. Thus, the Signer Certificate can be uniquely identified upon decoding the header.

2.2.2 Document Feature Definition Reference and Document Type Category

The combination of the *Document Feature Definition Reference* and *Document Type Category* identifies a specific set of rules, such as this specification. Future use cases can thus reuse the same bar code and header format, but reference different feature definitions (i.e. a reference defining the list of information included in the bar code) or document type categories. This allows to reuse existing codebases, simplifies implementations and increases interoperability.

Document Feature Definition References and Document Type Categories for visa and emergency travel documents are defined in Doc 9303-7 and Doc 9303-8, respectively.

2.3 Message Zone

Following the header is the message zone. The message zone consists of the digitally encoded document features, as specified in this Section. Any order of the document features is valid, as long as all mandatory document features are present.

Each document feature is preceded by

- a tag identifying the type of feature (one byte)

- the length of the feature (one byte to five bytes)

Depending on the Version Identifier (at start position `0x01` in the Header, cf. Table 1) two types of length encoding have to be distinguished.

- For version number 3 and below, the length MUST be directly encoded in 1 byte (this “length byte” is the 2nd byte directly after the “Tag” of the message).
- For version number 4 and above, the length MUST be encoded using DER-TLV according to [X.690].

For visa documents it is RECOMMENDED to use version number 4 (or higher) and thus DER-TLV length encoding. Usage of version number 3 (or below) and thus direct encoding of the length is valid but discouraged.

For ETD documents version number 4 (or higher) and thus DER-TLV length encoding MUST be used.

2.3.1 Digital Encoding of Document Features (Binary Encoding)

Document features are encoded in the following way. As building blocks, we consider the following basic types:

1. *Alphanum*: Strings of uppercase[1] alphanumeric characters (i.e. A-Z, 0-9 and space)
2. *Binary*: Sequences of bytes
3. *Int*: Positive Integers
4. *Date*: Dates

These basic types are converted to sequences of bytes as follows:

1. Strings of alphanumeric characters are encoded as bytes by C40 encoding (cf. Section 2.6).
2. Sequences of bytes are taken as they are.
3. For positive integers, their unsigned integer representation is taken.
4. A date is first converted into a positive integer by concatenating the month, the days, and the (four digit) year. This positive integer is then concatenated into a sequence of three bytes as defined in the point 3) above.

Example: Consider March 25th, 1957. Concatenating the month, date and year yields the integer `03251957`, resulting in the three bytes `0x31 0x9E 0xF5`.

A digital document feature is a sequence of bytes. It has the following structure:

tag | length | value

Here *tag* is an integer in the range `0-254dec` acting as an unique identifier of the document feature. Note that tag `255dec` is reserved to denote the start of the signature. *length* consists of one to five bytes according to DER-TLV length fields encoding. *length* denotes the length of the following value. *value* is a basic type converted to a sequence of bytes.

Example: Consider a document feature that encodes the string “VISA01” with assigned tag `0x0A`. The C40 encoded byte sequence (cf. Section 2.6) of length 4 is `0xDE515826`. The document feature is thus the byte sequence

1 The restriction to uppercase letters is due to the limited data capacity of a bar code.

0x0A04DE515826.

A specific use case must hence augment this definition by enumerating which document features must be present and which can be optionally present, define their tag values and allowed length ranges.

Additional features, i.e. features with unknown tags MAY be present, for example for optional use of the issuing entity. Such additional features MUST NOT use the tag of the additional feature field, or the tag of any other optional or mandatory feature. The presence of features with unknown tags SHALL NOT affect the validity of the bar code, if the signature is recognized as valid.

2.4 Signature Zone

The beginning of the signature zone is indicated by the signature marker that has the value 0xFF, encoded as one byte, followed by one byte to five bytes denoting the length (the number of bytes) of the signature using the DER-TLV length fields encoding scheme.

The input of the signature algorithm MUST be the (hash of the) concatenation of the header and the complete message zone, excluding the tag that denotes the beginning of the signature zone or the length of the signature. The signature zone contains the resulting signature.

Only hashing and signature algorithms defined in Doc 9303-12 SHALL be used. Due to the resulting signature size, ECDSA with a key length of at least 256 bit in combination with SHA-256 is (at the time this document was created) RECOMMENDED.

Applying the ECDSA signature algorithm results in a pair of positive integers (r,s). This signature MUST be stored in raw format in the seal. The bit length of r and s respectively corresponds to the key length. Thus, for example, for ECDSA-256, the length of r and s is at most 256 bit = 32 byte each. The signature MUST be stored by computing the unsigned integer representation of r and s, potentially adding leading zeros to fit r and s to their expected length (i.e. the key length), and appending the resulting value of s to the one of r. See Appendix B for a conversion between the ASN.1 and raw format of (r,s).

2.5 Padding

If the header, message and signature together do not fill the available space of the bar code, padding characters SHALL be appended after the signature. All relevant 2D bar code symbologies define methods for padding in their respective standard, and padding MUST follow that definition.

2.6 C40 Encoding of Strings

In order to save space in encoding alphanumeric characters and the filler symbol <, the encoding scheme C40 is used, as defined in [ISO/IEC 16022]. In the following we define how these definitions are used in the current setting. The following two definitions apply for document features and their digital encoding:

1. Strings consist only of upper case letters, numbers, <SPACE>, and the symbol '<'. The latter is used as a filler symbol for the MRZ of travel documents. If '<' occurs in the string, all occurrences of '<' are replaced by <SPACE> before encoding. A string MUST NOT contain any other symbols.

2. Given a string of length L, the length (i.e. the number of bytes) of the corresponding digital encoding is the least even number, that is larger or equal to L.

In the following calculations, a byte value and the corresponding unsigned integer equivalent are implicitly converted. For example, we define the value of a byte by a formula consisting of integer arithmetic on integer values.

2.6.1 Encoding

Encoding a string of characters into a sequence of bytes works as follows: First, the string is grouped into tuples of three characters, and each character is replaced with the corresponding C40 value according to Table 2, resulting in a triple `(U1,U2,U3)`. Then for each triple, the value

```
U = (1600 * U1) + (40 * U2) + U3 + 1
```

is computed. The result is in the range from 1 to 64000, giving an unsigned 16 bit integer value. This 16 bit value `I16` is packed into two bytes by

```
Byte 1 = (I16) div 256

Byte 2 = (I16) mod 256
```

Here `div` denotes integer division (no remainder), and `mod` denotes the modulo operation. Note that these operations can be implemented by bit-shifting.

Table 2: C40 Encoding chart and correspondence to ASCII

C40 Value	Character	ASCII Value	C40 Value	Character	ASCII Value
0	Shift 1	n/a	20	G	71
1	Shift 2	n/a	21	H	72
2	Shift 3	n/a	22	I	73
3	<SPACE>	32	23	J	74
4	0	48	24	K	75
5	1	49	25	L	76
6	2	50	26	M	77
7	3	51	27	N	78
8	4	52	28	O	79
9	5	53	29	P	80
10	6	54	30	Q	81
11	7	55	31	R	82
12	8	56	32	S	83
13	9	57	33	T	84

C40 Value	Character	ASCII Value	C40 Value	Character	ASCII Value
14	A	65	34	U	85
15	B	66	35	V	86
16	C	67	36	W	87
17	D	68	37	X	88
18	E	69	38	Y	89
19	F	70	39	Z	90

2.6.2 Decoding

The encoding can be easily inverted. Given a pair of bytes, let `(I1,I2)` denote their unsigned integer values. The 16 bit value `I16` is recalculated as

```
V16 = (I1 * 256) + I2
```

The triple `(U1,U2,U3)` can be recomputed by

```
U1 = (V16 – 1) div 1600

U2 = (V16 – (U1*1600) – 1) div 40

U3 = V16 – (U1*1600) – (U2*40) – 1
```

Here again, `div` denotes integer division. Characters can be decoded from the triple `(U1, U2, U3)` by simply looking up the corresponding values in Table 2.

2.6.3 Padding

The above definition is only well defined if the length of the string to be encoded is a multiple of three. Akin to the padding-definitions given in [ISO/IEC 16022], the following padding rules apply:

1. If two C40 (=two characters) values remain at the end of a string, these two C40 values are completed into a triple with the C40 value 0 (Shift 1). The triple is encoded as defined above.

2. If one C40 value (=one character) remains, then the first byte has the value `254dec` (`0xFE`). The second byte is the value of the ASCII encoding scheme of DataMatrix of the character corresponding to the C40 value. Note that the ASCII encoding scheme in DataMatrix for an ASCII character in the range 0-127 is the ASCII character plus 1.

3. DIGITAL SEAL USAGE

This section gives a generic description of the Digital Seal Usage, which applies to visa and Emergency Travel Documents. Specific requirements are defined in the corresponding profiles.

3.1 Content and Encoding Rules

3.1.1 Header

The encoding of the header for digital seals is according to Section 2.2.The value of the last 2 bytes for the *Document Feature Definition Reference* and the *Document Type Category* depends on the specific document profile. The Document Type Category must be an odd number for ICAO profiles. Even numbers MAY be used for national profiles not specified by ICAO.

3.1.2 Document Features Encoded in the Digital Seal

The document feature that MUST be stored in the seal is the Machine Readable Zone:

The digital seal SHALL encode the MRZ of a document. The MRZ may be of any of the types specified in Doc 9303. However, the specific document profiles MAY restrict the types of permissible types of MRZs.

Each document profile MAY define additional REQUIRED and OPTIONAL fields.

3.1.3 Encoding Rules for Document Features

The encoding of document features depends on the *Document Feature Definition Reference* in combination with the *Document Type Category*. Specific values are defined in the corresponding document profiles.

3.2 Bar code Signer and Seal Creation

To allow easy verification of digital seals, this specification leverages the existing CSCA PKI to issue and distribute certificates as well as CRLs. For details and certificate profiles, see Doc 9303-12.

3.2.1 Architecture of the Bar Code Signer System

The bar code Signer receives data from a Document Personalization System to encode a digital seal, and uses a signing key to sign it. Figure 2 depicts a possible implementation of the bar code Signer and its client, the Document Personalization System.

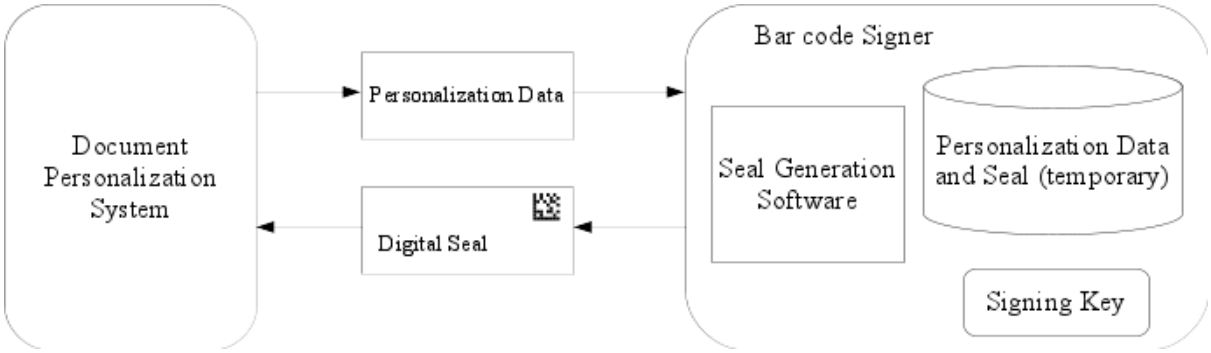


Figure 2: Document Personalization: Scenario with centralized bar code Signer

The bar code Signer relies on the following software and data:

- The *seal generation software* produces digital seals conforming to the present standard. It receives the personalization data sent by the client, signs these data with a private signing key, and encodes the personalization data and the signature to a bar code. The personalization data and the digital seal are the input and output data, respectively, of the seal generation software. This data must be stored temporarily in the bar code Signer during the generation of the seal.

- The *signature keys* (private and public key) are used to sign and verify a digital seal. The private signing key is the most critical data of the bar code Signer.

Depending on the deployment scenario, the distinction between the document personalization system and the bar code signer is not always strict. For example, the bar code signer can be part of the personalization system at an embassy. A possible scenario is extending the personalization system to include signature generation, and storing signing keys on a smartcard within an embassy. Another approach is to set up a central bar code signer in the home country, and let embassies connect to it via a secure channel. Last, some embassies might not personalize documents themselves; then the personalization system could be also set up at the home country and integrated with the bar code signer.

As it produces the signature, the bar code Signer is a very critical component. The signature allows to verify the integrity of the bar code data, i.e. whether the data have been manipulated, as well as their authenticity, i.e. whether they are issued by an authorized entity.

In order to achieve a sufficiently high security level, it is RECOMMENDED that the bar code Signer be a central service, and not deployed at embassies, unless operational, technical, or logistical reasons prevent a centralized deployment. This is in order to concentrate the security measures on a limited perimeter, while taking into account best practices for ensuring recoverability and business continuity. Private signature keys SHALL be stored securely by the bar code Signer.

3.2.2 Security of the Bar Code Signing System

The Bar code Signing System SHOULD be hosted and operated according to best security practices in the following areas: physical security; server and network infrastructure; system; development and support processes; access control; and operations security. If the bar code Signer is set up as a central service, it is RECOMMENDED to ensure compliance with [ISO/IEC 27002] on the perimeter of the bar code Signer in order to ensure compliance to these best security practices.

4. REFERENCES (NORMATIVE)

[ISO/IEC 16022]	ISO/IEC 16022 Information technology -- Automatic identification and data capture techniques -- Data Matrix bar code symbology specification, 2006
[ISO/IEC 18004]	ISO/IEC 18004:2006: Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification, 2015
[ISO/IEC 24778]	ISO/IEC 24778:2008: Information technology – Automatic identification and data capture techniques – Aztec Code bar code symbology specification, 2008
[ISO/IEC 27002]	ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management, 2013
[ISO/IEC 15415]	ISO/IEC 15415:2011: Information technology – Automatic identification and data capture techniques -- Bar code symbol print quality test specification – Two-dimensional symbols, 2011
[X.690]	ITU-T X.690 2008, DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS OSI networking and system aspects – Abstract Syntax Notation One (ASN.1) Information technology – ASN.1 encoding rules

Appendix A to Part 13

EXEMPLARY USE CASE (INFORMATIVE)

This section gives a general overview of using a digital seal to protect a non-electronic document. The specific use case considered here is the protection of a visa document, and depicted in Figure A.1. Whereas technical details may vary for other use cases, the same general principles apply.

The general workflow can be separated into three steps. As a prerequisite, Visa Signer Certificates (VSC's) have to be generated. Next, digital seals are generated, and then later validated.

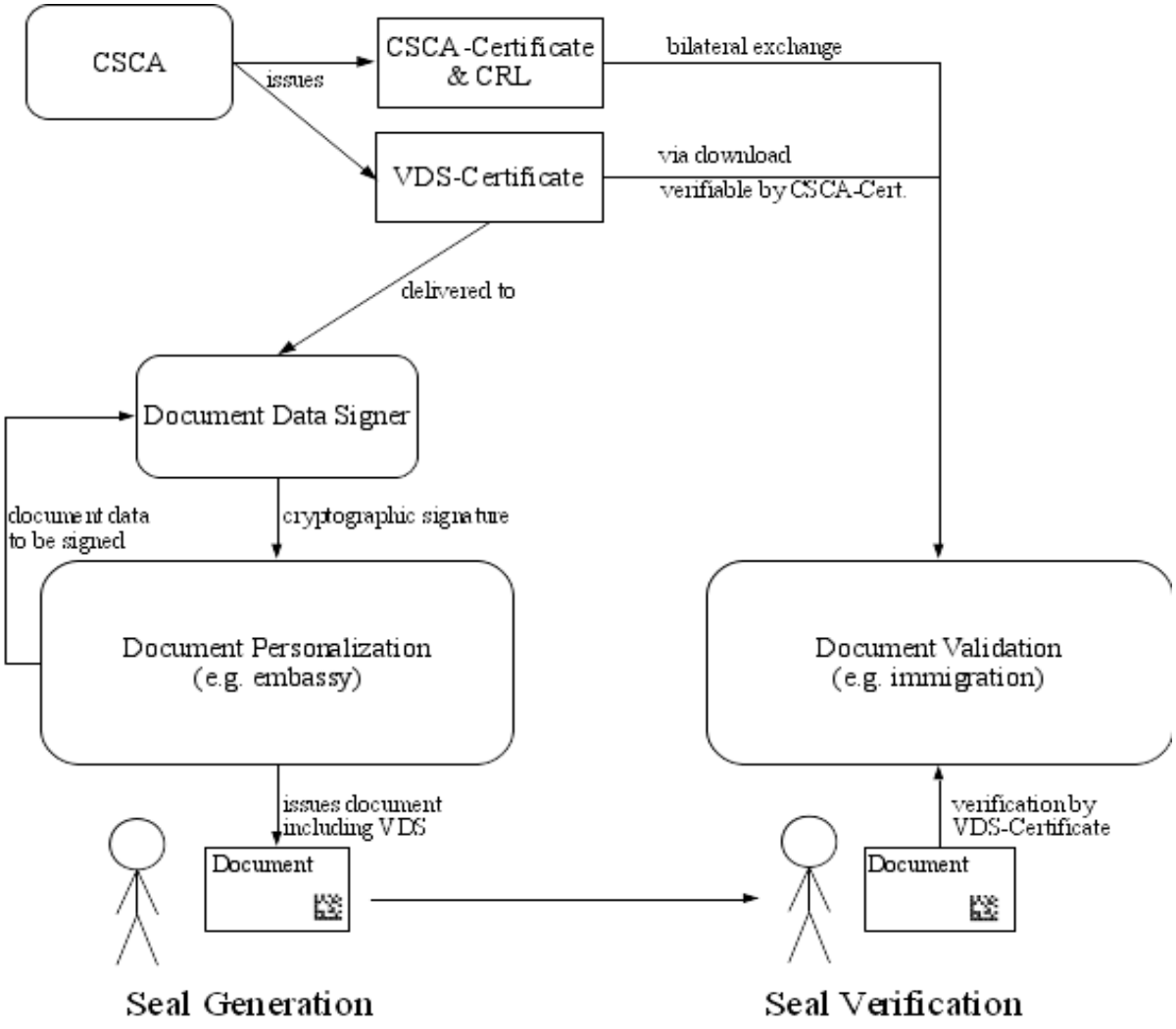


Figure A.1: Exemplary VDS Use Case

A.1 Prerequisite: Visa Signer Certificate Generation

The visa signing PKI is based upon the PKI set up for electronic passports defined by ICAO. At the root is the Country Signing Certificate Authority (CSCA) of each country. The CSCA publishes a CSCA-Certificate containing the public key of the CSCA. To enable trust between countries, this CSCA-Certificate is distributed in a trustworthy manner via bilateral exchange, or via master lists.

The Visa Signer is the entity that actually signs digital seals. Visa signer certificates are issued by the CSCA and can therefore be verified by the CSCA-Certificate

A.2 Digital Seal Generation

A digital seal is generated in two steps:

1. An applicant applies for a visa at the embassy where he resides. The embassy records the applicant's data and checks whether the applicant meets the requirements to receive a visa. If the requirements are fulfilled, the embassy sends a digital representation of the recorded data to the Visa Signer (VS). The VS can either be (1) a central entity located in the country that issues the visa, and the embassy connects to the VS via a secure channel, or (2) the VSs are decentralized entities placed at each embassy, for example using smartcards containing cryptographic keys that are directly attached to the personalization system. In any way, the VS cryptographically signs the recorded data.

2. For signing, the Visa Signer uses a key pair of a private key and a public key. The actual signing is done with the private key, whereas the public key is stored in a Visa Signer Certificate. The resulting signature is sent back to the Visa Personalization System if the Visa Signer is not a local part of the personalization system, printed on the visa sticker, and the visa sticker is attached to the applicant's passport.

A.3 Digital Seal Validation

When the applicant enters the issuing country, he presents his visa to a Visa Validation Authority (VVA), e.g. the immigration control of the issuing country. The VVA verifies the authenticity and integrity of the digital seal on the visa by validating the signature of the seal, and comparing the printed information on the visa sticker and on the passport with the digital information stored in the seal. The signature of the seal is verified by identifying the corresponding VS-Certificate with the help of the identifier stored in the header of the digital seal, and then using the public key of the VS-Certificate. As described in the previous paragraphs, the validity of the VS-Certificate itself can be verified by the CSCA-Certificate.

Remark
Since all certificates are publicly available, the validity of the visa can be verified by *any* third party, not just by the issuing state. The approach can thus handle use cases for unions of countries, where one country issues a visa for another country (as is done for example in the European Union). Another use case is verification of visas by airlines prior to boarding a plane.

Remark
The criteria to determine if a visa document can be trusted or not based on the digital seal and the MRZs of the visa and the passport are defined in a validation policy.

Appendix B to Part 13

CONVERSION OF ECDSA SIGNATURE FORMATS (INFORMATIVE)

B.1 Integer Encoding in DER/BER

Integers are encoded according to both the Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER) as the signed big endian encoding of minimal length, after which Tag-Length-Value (TLV) scheme is applied. We distinguish the following cases:

1. Suppose the integer value is positive, and the most significant bit (MSB) is zero in the minimal unsigned integer representation. Then the unsigned integer representation has the form below, which is the BER/DER value.

   `|0bbbbbbb| ...`

2. Suppose the integer value is positive, and the MSB is one in the minimal unsigned integer representation, i.e. has the form `|1bbbbbbb| ...` Then a byte containing zeros is put in front and the BER/DER value is

   `|00000000|1bbbbbbb| ...`

3. Suppose the integer value is negative. Then that value is encoded as the two's complement, for example by taking the unsigned minimal integer representation, inverting, and adding one. Afterwards the MSB is set to one. For example for -25357 we have the unsigned minimal integer representation

   `|0110 0011|0000 1101|`

   This is inverted to

   `|1001 1100|1111 0010|`

   One is added

   `|1001 1100|1111 0011|`

   and results in the BER/DER value. Note that the fact that the number is negative can be directly inferred by the fact that the MSB (here leftmost) is one.

Finally, one yields a TLV value by putting two bytes in front of the above encoded BER/DER values. The first byte is the tag with the constant `0x02`. The second byte contains the length (i.e. number of bytes) of the following encoded BER/DER value. Decoding can be simply done by e.g. distinguishing according to the MSB whether a negative or positive integer is encoded, and applying the above steps in reverse.

B.2 Example

Table B.1 gives some examples of DER/BER encoded integers.

Table B.1: DER/BER encoding examples for some integer values.

Value (dec)	Tag (hex)	Length (hex)	Value (hex)	Value (binary)
0	0x02	0x01	0x00	00000000
127	0x02	0x01	0x7F	01111111
128	0x02	0x02	0x00 0x80	00000000 10000000

Value (dec)	Tag (hex)	Length (hex)	Value (hex)	Value (binary)
-129	0x02	0x02	0xFF 0x7F	11111111 01111111

B.3 ECDSA signatures in ASN.1/DER

The ASN.1 description of an ECDSA signature is

```
Signature ::= SEQUENCE {
       r INTEGER, s INTEGER
}
```

This sequence is encoded according to DER as a TLV triple with tag `0x30`, the length as the number of bytes of the following value, and the value as the concatenation of the TLV triples of the encoding of `r` appended with the encoding of `s`.

Two example sequences – integers `r` and `s` of an ECDSA signature are of course much larger in practice – are given in Table B.2.

Table B.2: DER encoded sequences of two integers

Integers		TLV of Sequence		
R	**S**	**Tag**	**Length**	**Value**
127	1	0x30	0x06	0x02 0x01 0x7F 0x02 0x01 0x01
128	127	0x30	0x07	0x02 0x02 0x00 0x80 0x02 0x01 0x7F

Note that `r` and `s` are always positive integers for an ECDSA signature. Therefore to convert from a raw signature to DER, one has to first split the raw signature in half to get `r` and `s` individually, and then encode them as a DER encoded ASN.1 sequence according to the definition above. Conversely, to decode from an ECDSA signature in DER, one has to first decode the sequence, extract the unsigned integer representation of `r` and `s` and set both `r` and `s` to a fixed length (= length of key size) representation by stripping or adding leading zero bytes if required (e.g. in the case of ECDSA-256 both `r` and `s` must have a length of 256 bit = 32 byte), and appending the value resulting from `s` to the value resulting from `r`.

Appendix C to Part 13

EXAMPLES FOR C40 ENCODING (INFORMATIVE)

C.1 Example 1

Suppose the string “XK<CD” is to be encoded. By definition, all occurrences of '<' are replaced by <SPACE> before encoding. The resulting string is thus “XK CD”, i.e. “XK<SPACE>CD” (one space inserted). The C40 encoding/decoding of the string “XK<SPACE>CD” is depicted in Table C.1.

Table C.1: Encoding/Decoding example for the string “XK<SPACE>CD”.

Operation	Result			
original string	“XK<SPACE>CD”			
grouping into triples	(X, K, <SPACE>)		(C, D,)	
replacing with C40 values and padding	(37, 24, 3)		(16, 17, padding)	
calculating the 16 bit integer value	60164		26281	
	Byte 1 (div)	**Byte 2 (mod)**	**Byte 1 (div)**	**Byte 2 (mod)**
resulting byte sequence (decimal)	235	4	102	169
resulting byte sequence (hex)	0xEB	0x04	0x66	0xA9

C.2 Example 2

Suppose the “XKCD” is to be encoded. The string solely consists of uppercase letters. Its C40 encoding/decoding is depicted in Table C.2.

Table C.2: Encoding/Decoding example for the string "XKCD"

Operation	Result	
original string	“XKCD”	
grouping into triples	(X, K, C)	(D, ,)
replacing with C40 values and padding	(37, 24, 16)	(unlatch C40 and encode in ASCII)

Operation	**Result**			
calculating the 16 bit integer value	60177			
	Byte 1 (div)	**Byte 2 (mod)**	**Byte 1**	**Byte 2**
resulting byte sequence (decimal)	235	11	254	69
resulting byte sequence (hex)	0xEB	0x11	0xFE	0x45

Appendix D to Part 13

VALIDATION POLICY RULES (INFORMATIVE)

The Validation Policy is a set of validation rules that allow to determine the validity of the seal on the document. The application of this Validation Policy outputs a status indication with one of the following values:

1. *VALID.* The seal's authenticity and integrity has been confirmed. Here authenticity means that the data in the seal were indeed signed by a bar code Signer of the issuing country of the document, and the corresponding bar code Signer Certificate is valid. Integrity means that the data of the MRZ of the sealed document were not modified, and the digital seal was not swapped from the document on which it was originally attached to.

2. *INVALID*. The seal is not recognised valid, and further investigation is needed. Invalidity may occur due to the following three reasons:

    a) *Fraud/Forgery*. This includes unauthorized personalization of a document, based on a stolen blank sticker, changes of the personalization data of a document based on an original sticker, or swapping a bar code sticker from a stolen document (e.g. passport) to another one, or other falsifications.

    b) *Damage/Tear*. The bar code cannot be decoded due to wear, tear or stains.

    c) *Unknown and/or Unexpected Errors*. This includes unpredictable errors, for example due to bugs in the software implementation used for decoding, or erroneous encoding during personalization.

Attached to the status indication INVALID are status sub-indications. These indicate the reasons for the invalidity of the seal. Since the chance of a fraud is dependent on these reasons, it is recommended to map the status indications and sub-indications to the three trust levels “trustable”, “medium fraud potential”, and “high fraud potential”. The recommended mapping is illustrated in Table D.1.

This generic Validation Policy always considers the following questions:

1. Is the visible digital seal valid?

2. Is the MRZ of the document valid?

3. Does the MRZ of the document match with the visible digital seal?

Below we give the validation rules for each type of control, list the validation criteria, expected results for each criteria, and resulting status sub-indications.

Visible Digital Seal Validation

1. Format Validation

    - if the physical encoding format is not compliant with the specification, or if errors due to physical noise cannot be corrected, the status is INVALID with sub-indication READ_ERROR

    - if the encoding format (i.e. the seal structures consisting of header, message zone and signature zone, or the binary/C40 encoding) is not compliant with the specification, or

    - if values expected in the header are unknown, or

    - if a mandatory field in the message zone is missing, or

- if the format of a field in the message zone is not compliant with the specification of the version defined in the header, then the status is INVALID with sub-indication WRONG_FORMAT, otherwise continue.

- if an unknown field is present in the message zone, then the sub-indication UKNOWN_FEATURE should be set. The status indication will be VALID or INVALID depending on the validity of the signature verified in the steps below. Note that if the signature is valid, the presence of an unknown feature alone must not violate the validity of the seal however.

2. Signature Validation

    - if the bar code Signer Certificate referenced in the header of the seal is not present, the status is INVALID with sub-indication UNKNOWN_CERTIFICATE.

    - if the bar code Signer Certificate referenced in the header of the seal was not signed by the CSCA, or the signature verification fails, the status is INVALID with sub-indication UNTRUSTED_CERTIFICATE

    - if the bar code Signer Certificate contains a DocumentType-Extension and the content of the bar code contains a MRZ, and the document type of the MRZ is not contained in the DocumentType-Extension, the status is INVALID with sub-indication INVALID_DOCUMENTTYPE

    - if the bar code Signer Certificate referenced in the header of the seal is expired, the status is INVALID with sub-indication EXPIRED_CERTIFICATE

    - if the bar code Signer Certificate referenced in the header of the seal is revoked, the status is INVALID with sub-indication REVOKED_CERTIFICATE

    - if the signature verification of the header and message zone using the bar code Signer Certificate referenced in the header of the seal fails, the status is INVALID with sub-indication INVALID_SIGNATURE

    - otherwise continue

3. Issuer Validation

    - if the CSCA is not trusted by the bar code Validation System on its trust domain, the status is INVALID with sub-indication UNTRUSTED_CERTIFICATE, otherwise continue.

The above validation rules cover a comparison of the data stored in the seal against data stored on the MRZ of the document. On top of that, a manual inspection of those data that are stored in the seal and printed on the document, but are not present in the MRZ of the documents, could be conducted.

Table D.1: Recommended Trust Levels of the Document Policy

Status Indication	**Sub Status Indication**	**Trust Level**
VALID	-	*Trustable*
	UNKNOWN_FEATURE	
INVALID	READ_ERROR	*medium fraud potential*
	EXPIRED_CERTIFICATE	
	WRONG_FORMAT	*high fraud potential*
	UNKNOWN_CERTIFICATE	
	UNTRUSTED_CERTIFICATE	

Status Indication	Sub Status Indication	Trust Level
	INVALID_DOCUMENTTYPE	
	REVOKED_CERTIFICATE	
	INVALID_SIGNATURE	

— END —