



ICAO

MACHINE READABLE TRAVEL DOCUMENTS GUIDANCE DOCUMENT

HIGH-LEVEL GUIDANCE: EXPLAINING THE ICAO DIGITAL TRAVEL CREDENTIALS

Version – 1.0 | June 2024

ICAO TAG/TRIP

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

1. PURPOSE

The purpose of this document is to support a more general understanding of the ICAO Digital Travel Credential (DTC). This high-level guidance is targeted to officials/decision-makers, with a particular focus on passport issuing authorities and border entities.

It is recommended that audiences not familiar with the DTC concept leverage this high-level guidance as a steppingstone to the more detailed policy and technical documents developed by ICAO, and read published DTC documents as follows:

For information on what the ICAO DTC concept entails

1. High Level Guidance: Explaining the ICAO Digital Travel Credential (this document)
2. [Guiding core principles for the development of a Digital Travel Credential](#) (policy framework informing the development of DTC technical specifications)

For details on ICAO DTC technical specifications

3. [Technical Report: Digital Travel Credentials Virtual Component Data Structure and PKI Mechanisms](#)
4. [Technical Report: Digital Travel Credentials Physical Component and Protocols](#)

2. BACKGROUND

2.1 ICAO's Role

The International Civil Aviation Organization (ICAO) is a specialized United Nations agency directed by Member States to adopt air travel-related standards, practices and policies aimed at enhancing facilitation and security. Standardization is fundamental to establishing confidence in the reliability of travel documents and the efficient operations of border inspection and air travel processes.

2.2 The ICAO DTC Concept

The ICAO DTC is a secure and globally interoperable digital companion and/or substitution to a physical eMRTD, designed to support seamless travel.

A globally interoperable approach to travel documents presents many benefits to the passport holder, inspection authorities and industry stakeholders. **States seeking to deploy a digital companion and/or digital alternative to physical passports are strongly encouraged to leverage the ICAO DTC concept.**

The key feature of the ICAO DTC is that authorities can verify a digital representation of the passport data before the traveller's arrival and confirm the data's integrity and authenticity. The ICAO DTC can thus enable:

- Enhanced screening capabilities (travel authorization processing and pre-arrival screening) via the collection of accurate and trusted information, including facial biometrics, in advance of travel;
- Supporting increasingly efficient border processes by expanding automated and biometrically-enabled processes; and,
- Faster and more convenient experiences for travellers.

Finland's initial ICAO DTC-1 pilot findings reveal significantly faster border processing times, averaging less than 8 seconds, a notable efficiency gain in comparison to the 25 second typical average processing time of automated border kiosks.

2.2.1 Data Minimization and Selective Disclosure

While the ICAO DTC may be applicable to use-cases beyond border processing, such as digital identity systems, these applications are not within ICAO's remit and have not been addressed in the design and technical development of the ICAO DTC.¹ Accordingly, data protection concepts enabling the sharing of individual data elements (e.g., name, citizenship, date of birth, age, etc.) required to access a service do not apply to the ICAO DTC, which contains the full data set required to carry out the border inspection process (e.g., the biographic and document data outlined in the Machine Readable Zone and the facial biometric). Non-border control entities seeking to avoid the collection of unnecessary data, such as the facial biometric, could leverage the ICAO DTC to collect only the holder's biographic/document data (see section 6).

Note: The implementation of the ICAO DTC may introduce new risks. An overview of risks unique to the ICAO DTC is included in the [Guiding core principles for the development of a Digital Travel Credential](#).

3. WHAT DOES THE ICAO DTC ENTAIL?

3.1 ICAO DTC Components

The ICAO DTC combines physical and digital security features to support efficient and secure traveller processing. These features consist of the DTC Virtual Component and the DTC Physical Component.

Before the deployment of the eMRTD, passports were manually verified via physical security features. In addition to these physical security features, the eMRTD introduced digital security features that allow for the identification of fraud via electronic validation. These digital security features are leveraged in the ICAO DTC.

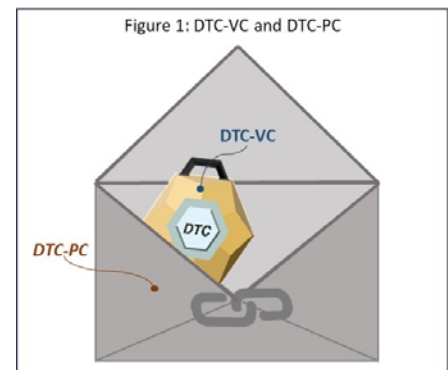
3.1.1 DTC Virtual Component

The DTC Virtual Component (DTC-VC) is the **digital representation of the passport's data**, cryptographically linked to the issuing authority (i.e. digitally signed by the issuer). Verifiers check the digital signature to confirm the credential is authentic and has not been altered.

3.1.2 DTC Physical Component

The DTC Physical Component (DTC-PC) is a carrier for the DTC-VC and serves as a **physical authenticator** (such as the process employed today to confirm the eMRTD personalized chip belongs to the book). There is only one DTC-PC for each DTC-VC, which is cryptographically linked to its DTC-VC (via digital signature), enabling verifiers to confirm a DTC-VC's link to its corresponding DTC-PC. From a functional perspective, the DTC-PC can be created on any form factors (i.e. devices) supporting DTC specifications (the issuing State or organization will need to ensure the chosen form factor meets its security requirements).

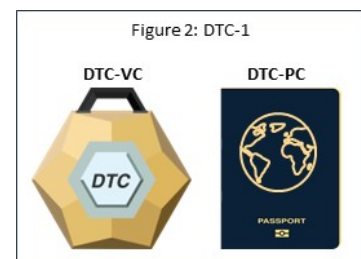
While the ICAO DTC is expected to enhance travel facilitation, travellers will still require physical passports for many years to come in order to meet State regulations and/or as a back-up option.



3.2 ICAO DTC Types

3.2.1 Overview

The ICAO DTC can be implemented in three different ways, each offering different options for issuers and verifying entities. ICAO DTC types are not hierarchical, nor do they represent evolving DTC solutions. Each ICAO DTC Type is comprised of a DTC-VC and a DTC-PC. All DTC Types leverage the same technical specifications for the DTC-VC, as outlined in the Digital Travel Credentials Virtual Component

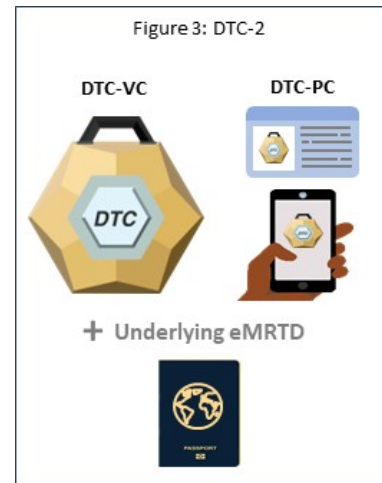


¹ The approach to DTC development endorsed by TAG/TRIP/4 is outlined in TAG/TRIP/4-WP/13 (Data Minimization) and TAG/TRIP/4-WP/14 (DTC Way Forward).

Data Structure and PKI Mechanisms Technical Report. Technical specifications for the DTC-PC – other than the underlying eMRTD – apply to the ICAO DTC Type 2 and Type 3.

3.2.2 Type 1 DTC (DTC-1)

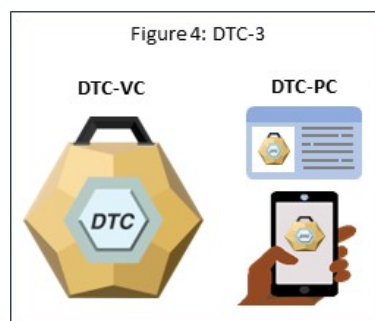
DTC-1 consists of a DTC-VC and the eMRTD serves as the DTC-PC. The digital representation of the passport data (DTC-VC) is derived from the Travel Document Issuing Authority's data (e.g., derived from the eMRTD chip). Because the DTC-1 originates from an existing eMRTD, it is considered to be issued by the passport authority. This ICAO DTC type is essentially a replica of the electronic data in the eMRTD chip, with the exception of other optional stored biometrics², and must be accompanied by the physical passport (i.e. the DTC-PC) during travel.



DTC-1 can be implemented at this time. Pilots funded by the European Union have confirmed the viability of the ICAO DTC concept, and are providing key implementation findings to be expanded on in ICAO's DTC-1 implementation guidance (under development).

3.2.3 Type 2 DTC (DTC-2)

The issuing authority creates a DTC-PC on any form factor supporting ICAO DTC technical specifications and meeting the authority's security requirements, and cryptographically links it to the embedded DTC-VC. Clients issued a DTC-2 would hold an underlying physical eMRTD that shares the same passport number as the ICAO DTC and can also serve as a physical component to the DTC-VC; accordingly, it is recommended that DTC-2 users carry their eMRTDs as back-up.



The form factor of the DTC-PC is at the discretion of the issuing authority. This paper outlines two examples: 1) contactless smart card format³ (mimics eMRTD inspection processes and protocols); and 2) mobile phone format (poses new security and processing considerations that may require changes to inspection systems).

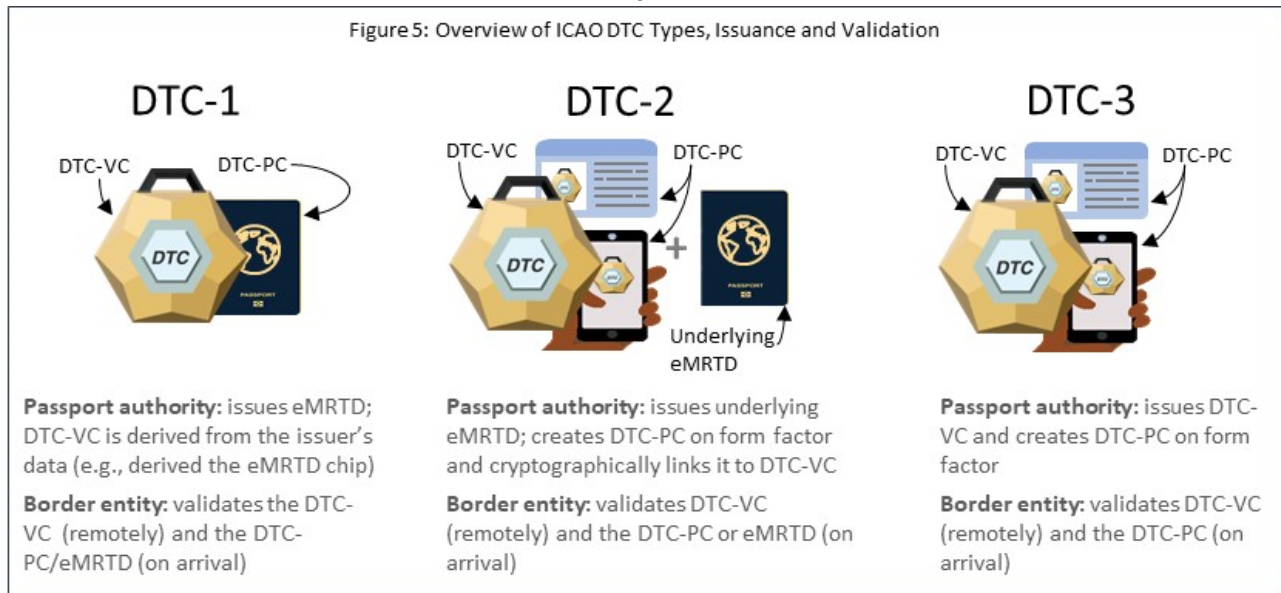
3.2.4 Type 3 DTC (DTC-3)

The passport authority issues the DTC-VC and creates the DTC-PC on a form factor, similar to the DTC-2. This ICAO DTC type is issued without an underlying eMRTD book and is currently being considered by some States as an option for emergency travel documents.

At this time, the DTC-2 and DTC-3 can be implemented on a contactless smart card (the most suitable option at present). See Appendix A for a detailed outline of ICAO DTC Types and a comparison to MRTDs and eMRTDs.

² See [Guiding core principles for the development of a Digital Travel Credential](#), clause 7.

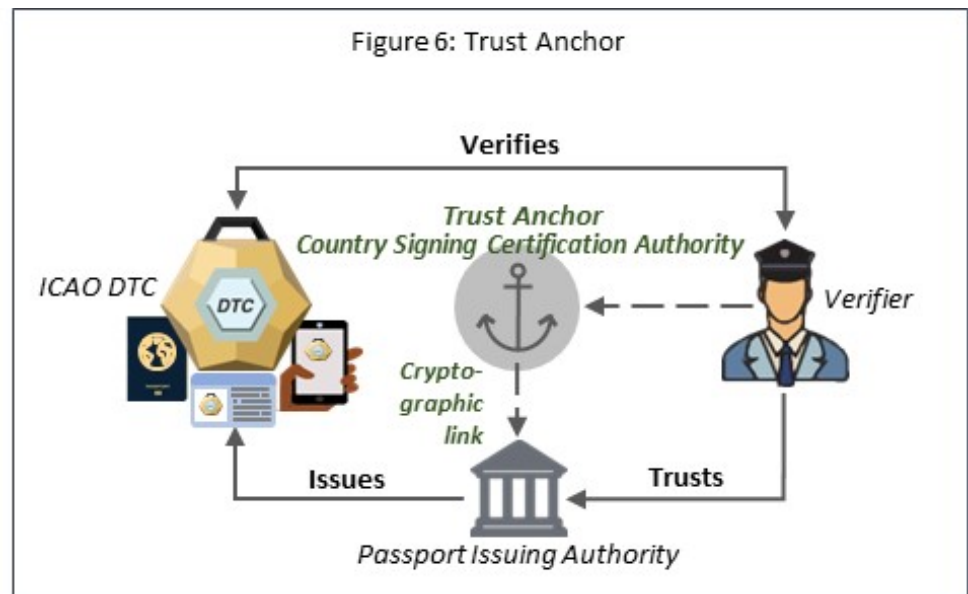
³ Doc 9303 Part 5 outlines specifications for TD1 size machine readable official travel documents (MROTDs).



4. WHAT DOES AN ICAO-COMPLIANT DTC ENTAIL?

An ICAO-compliant DTC must be successfully validated by the verifying entity – this is key to establishing confidence in the authenticity and integrity of the ICAO DTC, and hinges on the DTC maintaining an unaltered cryptographic link to the issuing authority (i.e. the passport issuer's digital signature cannot be altered and must remain the mechanism for verifying the DTC).

Altering the ICAO DTC or resigning individual data elements post issuance will break the chain of trust and challenge the integrity of the DTC. This cryptographic link is similarly employed in the eMRTD and encompasses a trust anchor for confirming that the travel document was issued by the identified issuing State or Organization.



While the ICAO DTC is designed for border inspection, it could be used outside its intended scope as a source document for verifiable identity information, including to access services/goods or to create other forms of digital credentials.

In Netherland's ICAO DTC-1 pilot, travellers derived ICAO-compliant DTC-1 credentials via a mobile application and used the credential to board the flight and cross border control upon arrival.

In cases where the ICAO DTC is converted to a different digital credential format or altered (e.g., introducing digital signatures not originating from the passport issuing authority), the credential is no longer considered an ICAO-compliant DTC.

Non-compliance with ICAO travel document specifications can hamper the functionality of travel documents, negatively impact border operations and undermine a State's or organization's investments in their travel documents. For the holder, it can also lead to refusal of entry.

5. ICAO DTC DEVELOPMENT ROADMAP

ICAO DTC development is led by the ICAO New Technologies Working Group (NTWG), in collaboration with the International Organization for Standardization (ISO), and guided by established [guiding principles](#). ICAO DTC specifications development is carried out in two phases:

PHASE 1 (COMPLETE) – The ICAO DTC behaves like an eMRTD book

This phase of work produced technical specifications for the DTC-VC and the DTC-PC on an underlying eMRTD (DTC-1) or a contactless smart card (most suitable implementation option for DTC-2 and DTC-3). See section 1 for links to published technical reports.

PHASE 2 (UNDERWAY) – Exploring new ICAO DTC protocols and interfaces

This second phase of work is exploring technical specifications that may enable the creation of the DTC-PC on a mobile phone, along with the assessment of new security considerations and inspection system engagement options. ICAO's Technical Advisory Group on the Traveller Identification Program endorsed the scope of ICAO DTC Phase 2 work, focussing on border processing, including the air travel scenario, in October 2023. See appendix B for further details on the development of the ICAO DTC.

ICAO Member State participation in this work is crucial to the successful implementation of the ICAO DTC. States are strongly encouraged to engage with the New Technologies Working Group and/or the Implementation and Capacity Building Working Group.

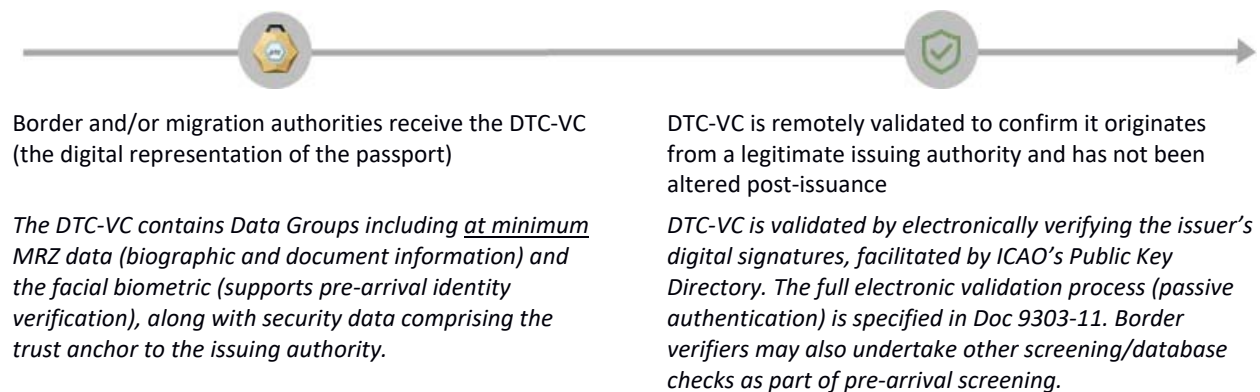
6. HOW CAN THE ICAO DTC BE USED?

6.1 Processing Travellers

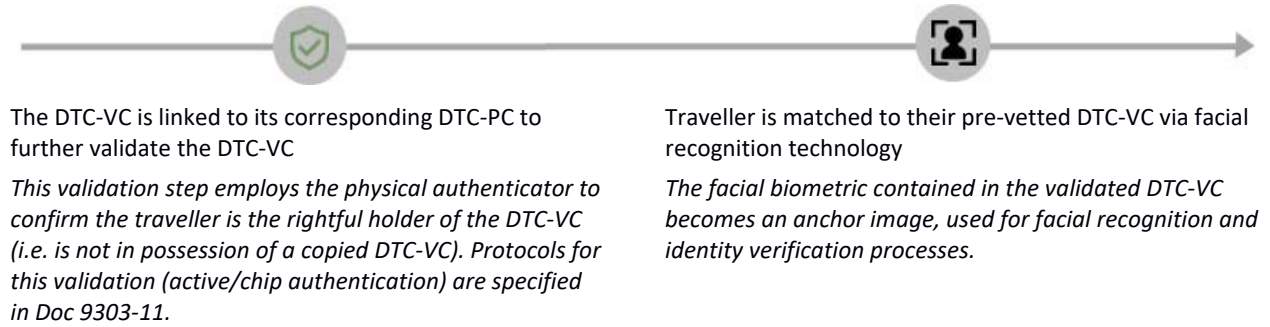
Overview for border and migration officials:

To ensure confidence in the authenticity and integrity of the DTC, it is recommended that the DTC receive the same level of scrutiny as the eMRTD. Authentication of both the DTC-VC and DTC-PC is strongly recommended.

Pre-Arrival



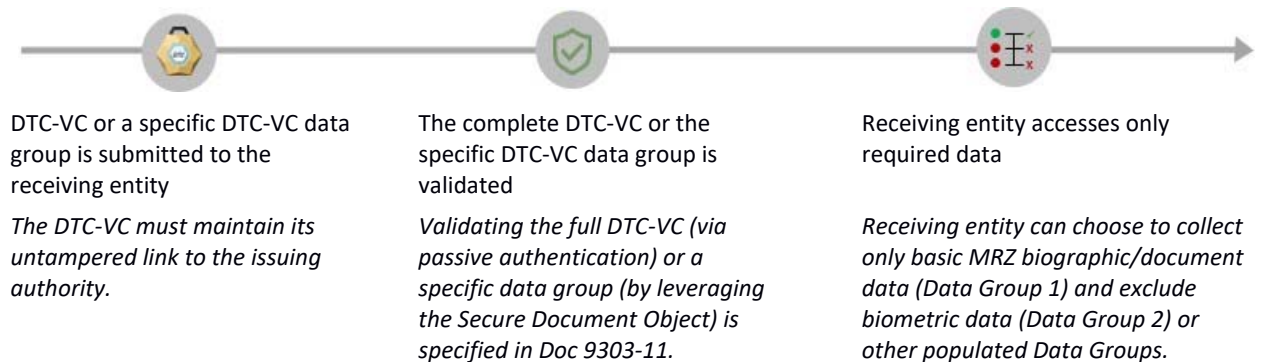
Arrival



6.2 Other Use-Cases/Processing






Overview for entities seeking to leverage the ICAO DTC as a source for verifiable identity information or access only biographic data:

Accessing select DTC data elements



In accordance with data protection and privacy principles, it is expected that the ICAO DTC may also be used as a verifiable source of identity information (i.e. a trusted identity document) by other digital identity schemes that disclose only the required data to access specific goods/services.

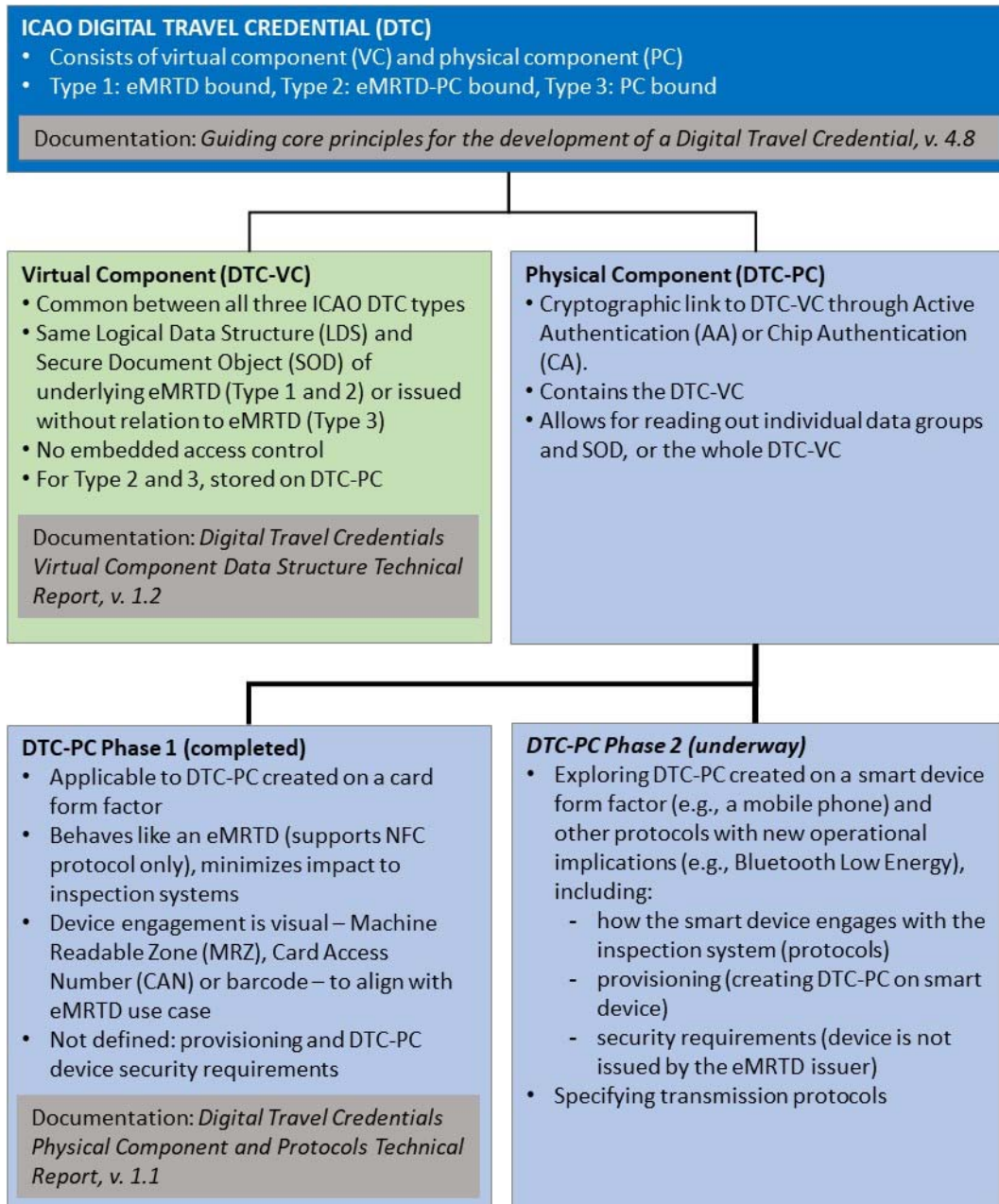
APPENDIX A
DETAILED OUTLINE: ICAO DTC TYPES

	MRTD 	eMRTD 	DTC-1 	DTC-2 	DTC-3 
Characteristics	Passport book with a Machine Readable Zone (MRZ)	MRTD book with an embedded chip	DTC-VC (derived from the Travel Document Issuing Authority's data, e.g., the eMRTD chip) and DTC-PC (eMRTD)	DTC-VC and DTC-PC (any form factor supporting technical specifications, such as card or mobile phone)	DTC-VC and DTC-PC (any form factor supporting technical specifications, such as card or mobile phone)
Passport book issued	Yes (MRTD)	Yes (eMRTD)	Yes (eMRTD)	Yes (eMRTD)	No
Relationship to physical passport book	N/A	N/A	DTC-VC is a copy of electronic eMRTD chip data (with the exception of optional secondary biometrics ⁴); eMRTD serves as authenticator	DTC-VC is a copy of eMRTD chip (with the exception of optional secondary biometrics ⁵); may include additional data elements	N/A – no underlying passport book
Physical authenticator	MRTD book	eMRTD book	eMRTD book	DTC-PC or eMRTD book	DTC-PC
Validity	5-10 years	5-10 years	Same validity as underlying eMRTD	Same or shorter validity than underlying eMRTD	Shorter validity than physical travel documents
Authentication/Validation	Manual or machine-assisted	Manual or machine-assisted and electronic validation of chip	Electronic validation of DTC-VC; confirm link to underlying eMRTD (both strongly recommended)	Electronic validation of DTC-VC; confirm link to DTC-PC and/or physical book (both strongly recommended)	Electronic validation of DTC-VC; confirm link to DTC-PC (both strongly recommended)
Status of technical specifications	Completed Doc 9303 – <i>Machine Readable Travel Document</i>	Completed Doc 9303 – <i>Machine Readable Travel Document</i>	Completed <i>Technical Report: Digital Travel Credentials Virtual Component Data Structure and PKI Mechanisms</i>	Phase 1 completed (applicable to DTC-PC created on card form factor) - <i>Technical Report: Digital Travel Credentials Virtual Component Data Structure and PKI Mechanisms</i> - <i>Technical Report: Digital Travel Credentials Physical Component and Protocols</i> See Annex B for information on Phase 2	Phase 1 completed (applicable to DTC-PC created on card form factor) - <i>Technical Report: Digital Travel Credentials Virtual Component Data Structure and PKI Mechanisms</i> - <i>Technical Report: Digital Travel Credentials Physical Component and Protocols</i> See Annex B for information on Phase 2
Annex 9 requirements:	Mandatory (Annex 9 Standard)	Recommended (Annex 9 Recommended Practice)	None (Optional)	None (Optional)	None (Optional)

⁴ See [Guiding core principles for the development of a Digital Travel Credential](#), clause 7.

⁵ See [Guiding core principles for the development of a Digital Travel Credential](#), clause 7.

A. OVERVIEW OF THE ICAO DTC AND SPECIFICATIONS DEVELOPMENT



Note: The capability to securely protect additional biometrics (fingerprint, iris data) are not subject to the DTC phase 1 and 2 specifications. Future generations of the DTC specifications may include the capability to securely protect additional biometrics.

APPENDIX B CONTINUED

B. BACKGROUND: POLICY POSITIONS INFORMING ICAO DTC TECHNICAL SPECIFICATIONS

<p style="text-align: center;">HYBRID CONCEPT</p> <p>The ICAO DTC is a combination of a virtual component and a physical component.</p>	<p>A hybrid approach to the ICAO DTC provides the advantages of both virtual and physical tokens and offers options to receiving entities (i.e. authenticate only the virtual component or perform additional verification of the physical component for increased security). The eMRTD can also be considered an example of a hybrid approach, as verifiers can choose to authenticate the chip or carry out additional checks to confirm the chip belongs to the passport book.</p>
<p style="text-align: center;">eMRTD MODEL</p> <p>The ICAO DTC builds on tried and tested eMRTD technical specifications and processes.</p>	<p>The ICAO DTC is meant to temporarily or permanently substitute a conventional passport with a digital representation of the traveller's identity. Existing eMRTD security properties provide a baseline for protecting the document from tampering and confirming the authenticity of the data/credential, including maintaining an untouched cryptographic link to the issuing authority.</p>
<p style="text-align: center;">SCOPE OF PHASE 1 AND PHASE 2 DEVELOPMENT</p> <p>Phase 1 ICAO DTC specifications development specified protocols that closely match the current border environment; Phase 2 work is exploring new interfaces.</p>	<p>Ensuring backwards compatibility (i.e., minimal disruptions to existing border inspection systems) is a key guiding principle for specification development. Accordingly, the technical reports developed during the first phase of ICAO DTC specifications development closely mirror how eMRTDs are processed at borders today. Phase 2 work is exploring other interfaces supporting the presentation of a mobile device to the inspection system, a potential new operational reality for the Type 2 and Type 3 ICAO DTC. While this guiding principle remains in place for the second phase of work, the NTWG is cognizant that these new implementation considerations may pose backwards compatibility challenges and other security-related considerations that will require further discussion by ICAO's Technical Advisory Group on the Traveller Identification Program (TAG/TRIP).</p>

APPENDIX C

GLOSSARY

Authentication/Validation	The process of validating the authenticity and integrity of an ePassport or ICAO DTC by verifying the digital signature.
Authenticators	Physical components that can be authenticated, i.e. ePassport, DTC-PC.
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 IC 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.
Cloning	Creating an exact digital representation/copy of an existing document.
Digital 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.
ICAO Digital Travel Credential (DTC)	Travel credential in a digital format that conforms with the specifications contained in ICAO DTC Technical Reports (and once incorporated, in Doc 9303) and is meant to temporarily or permanently substitute a conventional passport with a digital representation of the traveller's identity.
DTC Physical Component (DTC-PC)	The physical component of an ICAO DTC that is cryptographically linked to the virtual component.
DTC Virtual Component (DTC-VC)	The virtual component of an ICAO DTC containing the digital representation of the holder's identity.
electronic Machine Readable Travel Document (eMRTD)	An MRTD that has an embedded contactless integrated circuit, conforming to the specifications contained in Doc 9303 (commonly referred to as an ePassport).
ICAO Doc 9303	International specifications for Machine Readable Travel Documents.
ICAO New Technologies Working Group (NTWG)	Develops and updates travel document technical specifications for existing and emerging travel document technologies.
ICAO Technical Advisory Group/Traveller Identification Programme (TAG/TRIP)	The ICAO Traveller Identification Program (TRIP) develops, maintains and promotes international travel document specifications, standards and recommended practices. The main objective of TAG is to advise and support the ICAO Secretariat in the task of developing policy, recommendations and proposals for the implementation of the ICAO TRIP Strategy.
International Organisation for Standardisation (ISO)	The International Organisation for Standardisation is an international standard-setting body composed of representatives from various national standards organizations.
Interoperability	The ability of several independent systems or sub-system components to work together.
Issuing authority	The entity accredited for the issuance of an MRTD to the rightful holder. The Travel Document Issuing Authority issues the ePassport from which eMRTD Bound and eMRTD PC-Bound ICAO DTCs are created and validated. It is also the authority for data used to create and validate PC Bound digital travel credentials. This is the basis for the statement that an ICAO DTC must be issued by a Travel Document Issuing Authority.
Member states/contracting states	All countries that are affiliated with ICAO and comply with ICAO standards.
Passive Authentication	The process of authenticating the digital signature to confirm that the information stored on the chip or in the DTC-VC was saved by the proper authority (i.e. the passport issuer) and has not been tampered with.
Trust Anchor	In cryptographic systems with hierarchical structure this is an authoritative entity for which trust is assumed and not derived.