For Publication on the ICAO Website

# Guiding Core Principles for the Development of Digital Travel Credential (DTC)



**Version 4.4**

**October 2020**

File: Guiding Principles for the Development of Digital Travel Credential Specifications (DTC).doc

Author: ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP), Subgroup of the New Technologies Working Group (NTWG)

## 1. Purpose

The purpose of this policy paper is to:

1. Explain the Digital Travel Credential (DTC) concept.
2. Set out the guiding core principles for the development of the DTC .
3. Define the lifecycle related to the creation, management, validation and revocation of the DTC.
4. Explain differences in the risks of the DTC compared to the eMRTD.

## 2. Terminology

The key words "MUST", “MUST NOT”, "SHALL", “SHALL NOT”, "REQUIRED", "SHOULD", “SHOULD NOT”, "RECOMMENDED", "MAY", and “OPTIONAL” in this document are to be interpreted as described in [R1], RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. In case OPTIONAL features are implemented, they MUST be implemented as described in this Policy Paper.

## 3. Background

The New Technologies Working Group (NTWG) has established a sub group to standardise the issuance of travel credentials in a digital format. A DTC is intended to temporarily or permanently substitute a conventional passport with a digital representation of the traveller’s identity, which can in turn be validated using the travel document issuing authority’s public key infrastructure.

## 4. Guiding Principles

The policy position presented in this document is built-upon the core principles outlined below and is intended to inform the development of technical specifications.

The following core principles form the basis of the design of the DTC:

1. With respect to authenticity and integrity, the DTC MUST be at least as secure as an eMRTD
2. The information contained in the DTC MUST be derived from the Travel Document Issuing Authority’s data, and MAY come directly from the eMRTD.
3. The lifecycle management of the DTC may not necessarily be dependent on the lifecycle management of the eMRTD.
4. Changes MUST NOT be required in the current eMRTD standards or in the current process of issuing eMRTDs for authorities not intending to issue DTCs.
5. The revocation of a DTC MUST NOT result in the automatic revocation of the eMRTD associated with that DTC. This may be done procedurally at the discretion of the issuing State.
6. The revocation of the eMRTD MUST automatically revoke all underlying DTCs.
7. The DTC MUST be issued by a Travel Document Issuing Authority.

## 5. DTC Approach

The current security of the eMRTD results from the ability to verify the consistency of the data between the physical and the electronic document. The digitized data stored on the chip is identical to the printed information (the exception being the optional secondary biometrics and some special data groups) and ties the data on the chip to the holder of the document through a process of matching the primary biometric to the presenter of the Passport. Verification of the authenticity and integrity of the data is provided through Passive Authentication, and the OPTIONAL Active Authentication or Chip Authentication mechanisms bind the data

to the authentic chip. Comparison of digitized data stored on the chip to the printed information on the data page provides the binding with the secure physical document.

To ensure integrity and authenticity can be validated to the same level of security as an eMRTD, the DTC approach is based on a 'hybrid' concept, in which the DTC will consist of a Virtual Component (DTC-VC) containing the digital representation of the holder's identity and one Physical Component (DTC-PC) that is cryptographically linked to the Virtual Component. The DTC-VC does not have any copy protection or access control protection as it is a simple file structure.

The DTC can be implemented in three types:

a) Type 1 - eMRTD bound DTC – consist of a DTC-VC only, with the eMRTD as a physical authenticator

- The virtual component is an exact copy of the electronic document data, with exceptions noted in section 7
- In accordance with the guiding principles in section 4, an eMRTD bound DTC is considered to be issued by a Travel Document Issuing Authority, because it is derived from the Authority's data
- The traveller MUST have their physical eMRTD in their possession while traveling

b) Type 2 - eMRTD- PC bound – consists of DTC-VC and an DTC-PC in addition to the eMRTD

- The physical device serves as the DTC-PC, with the eMRTD as the alternate or as a fallback
- The virtual component will be an exact copy of the electronic document data, with exceptions noted in section 7
- The VC contains a link to the physical component
- The VC may contain additional data at the discretion of the issuing authority
- The traveller SHOULD have their physical eMRTD in their possession while traveling

c) Type 3 - PC bound – consists of a DTC-VC and a DTC-PC but NO eMRTD

- Only the physical device will serve as the DTC-PC
- The virtual component will use the exact same data elements as defined in the logical data structure of Doc. 9303, with exceptions noted in section 7.
- The VC may contain additional data at the discretion of the issuing authority
- There SHALL be a distinguishable identifier to recognise the document as a virtual credential without an eMRTD as an alternate or as a fallback
- May have its own document characteristics (ID [passport] number, validity period, digital signature, etc).

## 6. Life Cycle of a DTC

### 6.1. Creation

A DTC can be created in the following three ways:

a) Type 1 - eMRTD-bound (formerly known as 'Self-Derived DTC'): The DTC-VC is derived from an existing travel document.

b) Type 2 - eMRTD PC bound (formerly known as 'Authority-Derived DTC'): The DTC-VC is derived from an existing travel document. In this case, the DTC-VC MUST be signed by the issuing authority's public key infrastructure to support data authentication. The physical component of the DTC-PC will be created by the issuing authority on a physical device that may be supplied by the issuing authority or by the holder. The issuing authority should provide security and interoperability requirements for the physical device. The eMRTD PC bound DTC may be issued at the same time as the eMRTD, or at a later date within the validity period of the underlying eMRTD.

c) Type 3 - PC-bound DTC (formerly known as 'Authority-Issued DTC'): In this case, the DTC-VC MUST be signed by the issuing authority's public key infrastructure to support data authentication. The physical component of the DTC-PC will be created by the issuing authority on a physical device that may be supplied by the issuing authority or by the holder. The issuing authority should provide security and interoperability requirements for the physical device. Once a PC bound DTC has been issued, an eMRTD with the same document number MUST NOT be issued.

### 6.2. Validity of a DTC

eMRTD PC bound (Type 2) and PC bound (Type 3) DTCs will have a validity period attached to them. In the case of an eMRTD-PC bound DTC, it is RECOMMENDED that the validity period be shorter than the underlying eMRTD, but SHALL NOT exceed the validity period of the underlying eMRTD. This is to accommodate the expected short life-cycle of the associated DTC-PCs.

### 6.3. DTC Identifier

eMRTD PC bound (Type 2) and PC bound (Type 3) DTCs will have a unique identifier associated with them. In the case of the eMRTD PC bound, this will be different from the document number contained in the DTC-VC in Data Group 1 (DG1). The issuing authority can define its own numbering scheme in accordance with Doc 9303.

### 6.4. Use of a DTC

The DTC-VC can be used by the traveller to make travel more efficient. The DTC-VC can be submitted by the traveller in advance of travel to provide advance passenger information (API) and passenger name record (PNR) information, apply for authorizations, support pre-border risk-management, and prepare the airport for seamless flow.

In the process of travel, the DTC-VC can be used to facilitate the passenger through the travel continuum by successful matching to the biometric information included in the validated (using Passive Authentication) DTC-VC, and, if required, the DTC-PC can be presented on request to provide additional assurance of the link (by mechanisms provided by the DTC-PC) to the identity contained in the DTC.

The DTC-PC is used to bind the DTC-VC to a dependable source (e.g. authentic travel document, provisioned device, etc.) in possession of the traveller to provide the verifying authority with confidence that the traveller presenting themselves is authorized to use the associated DTC-VC. Technical specifications developed to support the DTC types should ensure that issuing or verifying authorities can determine whether a DTC-VC is linked to a DTC-PC in the rightful possession of the traveller.

To minimize risks and ensure consistency with the existing approach (i.e. one passport for one person), issuing authorities should only provision <u>one</u> DTC-PC per DTC-VC. Provisioning just one DTC-PC would allow issuing authorities to maintain control over reporting processes and provide the incentive for travellers to report their lost, stolen or decommissioned smart devices to the issuing authority.

If the device hosting the DTC-PC also holds the DTC-VC, but the holder does not want to submit their DTC-VC in advance, they may be able to present their smart device to the inspection equipment as a substitute for a physical document. Information stored in the DTC-VC could be read-out from the smart device and be used to biometrically match the holder to their credential.

To protect the privacy of the holder and the data transaction, the physical device must have protection against unauthorized use

### 6.5. Invalidation/Revocation

Like a regular travel document, issuing authorities can invalidate a DTC by reporting it to the appropriate domestic and international authorities. DTCs that are lost, stolen, revoked or cancelled are no longer valid for travel. Issuing authorities can invalidate a DTC by reporting the issued eMRTD (which has been derived from a record) lost, stolen, revoked or cancelled. The invalidation of the source authorization would automatically invalidate all DTC-VCs linked to that eMRTD.

eMRTD bound or eMRTD-PC bound DTCs share the Document Number with an existing eMRTD. Thus, revocation of the existing eMRTD also revokes the DTC. PC bound DTCs do not share the document number with any eMRTD, thus, the PC bound DTC must be revoked on its own.

## 7. DTCs and Biometrics

The DTC-VC will include only the facial biometric of the traveller stored in data group 2 to support traveller identification.

### 7.1. Other Stored Biometrics

Other [protected] biometrics held in data groups 3 and 4 will be omitted from the DTC-VC, as these are secured on the integrated circuit using more advanced computing chip capabilities. Attempting to port these over to the DTC-VC would present challenges for both issuing and validating authorities.

When an issuing authority has stored and protected other biometrics on the eMRTD chip, their hash values will be present in the security object. These biometrics will not be included in the DTC-VC, which will require inspecting authorities to handle these credentials in the same way that they would with an eMRTD where access to biometrics stored in these fields is not permitted.

If a country is storing (or considering storage) biometrics in data groups 3 and 4 without extended access control, these biometrics could be included in the DTC-VC of the traveller.

### 7.2. Biometrics and Future DTC Generations

Future generations of the DTC could include the capability to securely protect additional biometrics.

## 8. Best Practices

As the DTC and eMRTD are very similar except the form factor, verification of a DTC by a receiving entity requires the same procedures and the same levels of inspection scrutiny as for an eMRTD. Therefore, the potential risks resulting from the use of a DTC are largely similar or identical to those using an eMRTD. The following are suggested best practices to mitigate the risks:

- Prevent unauthorized access to the virtual component during transmission or storage
- Use Passive Authentication and verify the issuing authority is a trusted entity (state).
- Check that virtual component is not an unauthorized copy by verifying the physical component.

## 9. Risk Analysis

Many risks associated with DTCs are shared with eMRTDs. However, there are some core risks that are unique to the DTC. The following table lists risks associated with a DTC. It also differentiates between risks that are shared with eMRTDs and those that are unique to DTCs, and suggests some mitigation strategies for these risks.

| Scenario | Impact | Unique to DTC | Mitigation |
|---|---|---|---|
| Relying solely on DTC-VC without using the DTC-PC | Relying solely on a biometric match to the image in the DTC can lead to lookalike fraud | Yes | To reach a strong binding of travel credential and traveler, two factors need to be authenticated:<br>1. The verification of the possession of the DTC-PC or eMRTD by the traveler (e.g. via Active/Chip Authentication, checking the physical security features, or DTC-PC specific algorithms).<br>2. The biometric comparision of the biometrics contained in the DTC-VC and the traveler (including verification of authenticity via Passive Authentication)<br>Additionally, the link between DTC-VC and DTC-PC/eMRTD must be checked.<br>Based on the risk assessment of the verifier one of the factors might be left out, resulting in a weaker binding. This allows for flexibility in the verification of the DTC. |
| DTC enrolled to a device of an unentitled traveler | An imposter could assume the identity of the entitled traveller, pose security risks to international air travel, and/or contribute to other criminality (e.g. human trafficking, human smuggling, money laundering, terrorism, etc). | Partially.<br>This is the same as the issuance of an eMRTD to an unentitled traveler. However, the provisioning of the DTC-PC may be on a device that is already in the possession of the holder (for example, a smart device) and the issuer may not have ownership or control over the device. The provisioning process may also not be entirely within the infrastructure owned/controlled by the issuer. | Mitigating the risks of unentitled enrollment could be managed by the travel document issuing authority in the following ways:<br>1. Requiring in-person enrollment; and/or<br>2. Requiring a 1-to-1 biometric match [using facial recognition] to support enrollment; and/or<br>3. Tying enrollment to other national programs (e.g. digital identity, etc.). |
| Collection of DTC-VC data | The DTC-VC is just a file. So, criminals could collect DTC data to find a match for lookalike fraud. | Yes. | The threats associated with this risk could be mitigated in the following ways:<br>1. Secure communication channel between the smart device and inspection equipment; and/or<br>2. Education by issuing authority to prevent free distribution and appropriate protection of the DTC-VC; and/or |

| | | | |
|---|---|---|---|
| | | | 3. Where confidence in the identity of the traveller is needed perform second factor authentication<br>4. User consent before transmitting the VC<br>5. Ensuring that travel document holders are aware of and using channels to report compromised DTCs. |
| Provisioned DTC-PC is Lost by/Stolen from the Entitled/Documented Traveller. | A lost DTC-PC could be used for lookalike or imposter fraud. | No.<br><br>This is the same as losing an eMRTD. | The mitigation steps for the loss of a DTC-PC are the same as for the loss of an eMRTD. This is revoking the DTC, similar to the revocation of the eMRTD, by reporting it to the Interpol SLTD.<br><br>However, there is a chance that travelers are more likely to report the loss of an eMRTD than the loss of a device. Additional mitigation steps for DTCs could be the following:<br><br>1. Communication campaigns to ensure that travellers are aware of the risks associated with holding a DTC-VC on a DTC-PC; and/or<br>2. Encouraging DTC holders to register their devices to assist in DTC management; and/or<br>3. Limiting the validity of the DTC. |
| The keys of the DTC-PC are extracted | Extraction of the DTC-PC keys allows for duplicating the DTC-PC. This enables lookalike fraud by using the cloned DTC-PC | No.<br><br>This is similar to extraction of AA/CA keys from the eMRTD. However, there is one difference. The eMRTD data page has additional security features, which will also act as a check against cloning. | The threats associated with this risk could be mitigated in the following ways:<br><br>1. Establishing security requirements for the hardware and certification; and/or<br>2. Communication with DTC holders. |
| Not reporting Lost/stolen/decommission DTC-PCs | The impact is similar to the loss of and eMRTD | Partially.<br><br>Travellers may be less likely to report loss of a smart device hosting the DTC-PC to an issuing authority, and are highly unlikely to advise the issuing authority if they change smart devices (which will retain a DTC-PC on the security object of the decommissioned device). | Apart from educating travelers, it is advisable to issue short validity DTCs, and each request for the issuance of new DTC should involve a check to see if there is an existing one. It is important that travelers understand that a DTC may have a unique identity (i.e., not linked to an existing eMRTD), and that it should be reported if it lost or stolen. |
| Inspection system outage or failure of the DTC-PC device | In the case of the PC Bound DTC, if either the DTC-PC or the | Yes. | None |

| | | | |
|---|---|---|---|
| | inspection system has an outage, there is no fallback to a "physical" document | For PC-Bound DTC | |
| False rejection | The travel of a document holder could be significantly disrupted if there is a false rejection during facial recognition. With no fallback, a traveler could be falsely deemed unable to board a flight or enter a country. | Yes.<br><br>For PC-Bound DTC | None |

## 10. Other Considerations

### 10.1. Diplomatic, Official and Other Passports

The use of the second character [in the machine-readable zone] to denote a specific type of passport is not yet standardized, resulting in poor uptake and/or inconsistent practices. In most cases, issuing authorities will issue other travel documents (e.g. diplomatic, service, refugee travel documents, etc.) and populate the first character with 'P' to indicate that it is a passport. Limited use of the second character [in the machine readable zone]* combined with less human interaction (and the ability to visually identify these documents), could result in holders of these documents attempting to travel without the appropriate authorizations (e.g. visas, e-visas, etc.).

The lack of physical characteristics (i.e. red, green or black covers for passport books) to differentiate a DTC based on a regular passport from a DTC issued based on other passports presents challenges. If there are specific visa requirements for holders of these documents, issuers may decide to limit the issuance or creation of DTCs for this group.

* Recognizing the potential impacts of the lack of standardization for the second letter character of the machine-readable zone, the ICAO NTWG is conducting a feasibility study to determine if/when standardization may be possible.

### 10.2. Visas

The DTC will only include Logical Data Structure 1 (LDS1) (i.e. identity of holder and document information). The absence of other data – namely visas and travel history – could take-away from traditional risk management activities performed by Border and other authorities when determining whether to board or admit a traveller. Where a traveller does have a required physical counterfoil in their passport, they will need to carry, and at some points during the journey, present their document to the inspecting agent. Following a verification of the visa, these travellers could still benefit from seamless flows developed to support use of the DTC.

While Logical Data Structure 2 (LDS2) does open new possibilities to digitally store visa and travel history information, the first-generation DTC will not include functionality to support LDS2 data.

### 10.3. Storing multiple DTC-PCs on a single physical device

It is possible for multiple DTC-PCs to be hosted on a single physical device. However, if this option is exercised, then all potential exploitations of vulnerable groups (e.g. children, etc.) should be carefully considered.

## 11. Implementation Plan

The order in which DTCs specifications will be developed is as follows:

1. DTC-VC
2. DTC-PC

Once the DTC-VC is specified and endorsed, it can be used to issue eMRTD bound DTCs. Once the DTC-PC is specified and endorsed, it can be used to issue all types of DTCs.

## 12. Recommendations

The DTC sub group recommends that the ICAO TAG/TRIP endorse this policy paper at their meeting in July 2020.

— — — — — — — —

# Annex A

## USE CASES

### DTC-VC as an Enabler of Seamless Travel

Several industry initiatives around seamless travel involve the use of biometric (facial recognition) matching for a "touchless" interaction with the traveler. Each of these initiatives involves creating a package of verifiable traveler information with an anchor image that can be used for FR matching.

An eMRTD contains such an anchor image in Data Group 2, which has been authenticated by the issuer of the eMRTD. Since a DTC-VC contains the same information as present in the eMRTD's chip, a DTC-VC provides a globally interoperable package of verifiable traveler information that can be used as the basis for such initiatives, which allows for interconnects between the various seamless travel initiatives.

Both type 1 and type 2 DTCs are suitable for this. Type 1 DTCs (DTC-VC) can be created by reading the contents of the eMRTD chip at any point of the travel continuum. Type 2 DTCs have to be created by the issuer and has the added advantage that a higher resolution image of the holder can be included in the DTC. This improves the quality of the FR match.

### DTC to Improve the Advance Travel Authorization Process

Many countries have implemented Digital Travel Authorization regimes (alternatively called Electronic Travel Authorization, Electronic System for Travel Authorization, eVisa etc) which rely on the traveler providing biographic and biometric information to obtain permission to enter the country. In most cases, a photocopy of the passport data page is part of the submission.

Using the DTC-VC for such processes has the advantage of being able to authenticate the data and helping eliminate data entry errors. Both type 1 and type 2 DTCs can be used in this scenario.

### DTC to Streamline Border Management

Countries are increasingly investing in technology or processes that allow them to "push the border out". More and more, states are attempting to implement programs that initiate the border management process long before the traveler actually arrives in their destination country. The DTC-VC, sent in advance of the traveler arriving at the border enables authorities to conduct scenario-based targeting, watchlist lookup etc.

At the border, binding of a DTC-VC received in advance to the DTC-PC (initially an eMRTD for type 1, but in future a separate physical component/device) can be done by cryptographic means with an improvement in processing time due to advance receipt of the DTC-VC. Both type 1 and type 2 DTCs are suitable for this.

For industry, using the DTC-VC for the transmission of Advance Passenger Information (API) to Border has the advantage of being able to authenticate the data and helping eliminate data entry errors.

### DTC as an Emergency Travel Document (ETD)

DTCs have the potential to simplify the issuance of ETDs once the specifications of the DTC-PC have been completed. If a secure process for remote provisioning of the DTC-PC could be specified, it will be possible for countries to issue type 3 DTCs to their citizens who may have lost their travel document, to enable them to return home or travel to a location where they could apply and get a regular travel document.

— — — — — — — —

## Annex B

### FREQUENTLY ASKED QUESTIONS ON DIGITAL TRAVEL CREDENTIALS

| |
|---|
| ***What is a DTC?*** |
| A DTC is a digital representation of the traveller's identity which can temporarily or permanently substitute a conventional passport. The DTC operates in a similar way to the ePassport within the travel continuum, and can be validated using the travel document issuing authority's public key infrastructure.<br>The current ePassport securely binds its holder's information stored in the passport biodata page, to the chip inside the book. This information in the chip is stored in a Logical Data Structure (LDS) that must conform to ICAO Doc 9303.[1]<br>The DTC securely links the LDS in an issued ePassport as a virtual component (credential), and can also securely link the LDS to a physical component (authenticator) other than an ePassport (e.g. a mobile device). |
| *What is an authenticator?* |
| This is the DTC physical component or 'token'.<br>Authentication (usually referred to as ePassport validation in the current border process) is the process of validating the authenticity and integrity of an ePassport by verifying the digital signature of the stored data on the chip.<br>The token could be any physical 'cryptographic' device (such as a smartphone or a FIDO token) that is able to be authenticated in the same way the chip in the ePassport is authenticated. However, given that the physical security features of the ePassport book are not present then the device must be able to perform active (AA) or chip authentication (CA) ) or any equivalent mechanism. |
| *If we have a DTC will we still need to issue a physical passport?* |
| Yes, for the foreseeable future with two possible exceptions:<br>• For the facilitation of emergency travel (ETDs)<br>• Where a multi/bilateral agreement between Member States exists for specific 'trusted traveller' type programmes. |
| *Why has ICAO standardised the DTC?* |
| ICAO recognises that traveller behaviour and expectations are changing, global traveller volumes are growing rapidly; and there are an increasing number of proprietary global passenger facilitation schemes for digitising the ePassport. The absence of consistency in international deployment of such schemes has limited the opportunities to harmonize and build a global approach to traveller facilitation. Through specifications provided by ICAO, international civil aviation actors can ensure air traveller facilitation with a DTC aligns with the requirement for global interoperability. |
| *Who issues the DTC?* |
| A DTC can only be issued by a Travel Document Issuing Authority. That means a DTC is issued only on the basis of data created or held by a Travel Document Issuing Authority. The DTC in its three types (see below) can be seen as an extension of a State's sovereign travel document issuance powers. Accordingly, a DTC cannot be issued using data sourced from anywhere except the issuing authority. Also, an existing DTC cannot be taken and 'recreated' as a new credential by another issuing authority. |

[1] https://www.icao.int/publications/pages/publication.aspx?docnum=9303

**How can a DTC be created?**

There are three DTC types:

1. **eMRTD Bound (Type 1):** The DTC-VC is **derived from an existing travel document**. The traveller's current ePassport will act as their physical component (DTC-PC). This will mean that that traveller will still have their physical eMRTD (ePassport) in possession whilst travelling and the virtual component (DTC-VC) will be an exact copy of the data on that ePassport.
2. **eMRTD PC Bound (Type 2):** The DTC-VC is **derived from an existing travel document** with the option to store the DTC-VC in a remote system (e.g. database, web service) or store it elsewhere (e.g. smart device). The virtual component (DTC-VC) MUST be signed by the issuing authority's public key infrastructure (PKI) to support data authentication. The physical component (DTC-PC) will be created by the issuing authority on a physical device (i.e. a smartphone).
3. **PC Bound (Type 3): The issuing authority creates** a DTC and again has the option to store the DTC-VC in a remote system and store it elsewhere or the issuing authority could create the DTC and store it solely on this device. Again, the DTC-VC MUST be signed by the issuing authority's PKI. The physical authenticator of the DTC will be created by the issuing authority on a physical device. The issuing authority should provide security and interoperability requirements for the physical device. **Only** the physical device will serve as the DTC-PC.

*Where is the DTC stored?*

As it consists of two components (physical and virtual), the DTC can be stored in different form factors. At least one of these has to be a physical authenticator (DTC-PC). The physical authenticator of the DTC may be supplied by the issuing authority or by the holder. The issuing authority should provide security and interoperability requirements for the physical authenticators. The physical authenticator must be capable of providing active or chip authentication) or any equivalent mechanism.

*What benefits does the DTC provide?*

In addition to bringing the same benefits as the ePassport in reliably confirming the identity of the holder, the DTC can be used by the traveller to make travel more efficient. The DTC-VC can be submitted by the traveller in advance of travel to provide advance passenger information (API) and passenger name record (PNR) information, apply for authorizations, support pre-border risk management, and prepare the airport for seamless flow. In the process of travel, a passenger would use their DTC-VC by successfully matching to the biometric information included in the token, and, if required, presenting the DTC-PC when requested. The DTC can:

- Make travel more efficient through the improvement of passenger flows by allowing travellers to provide their data in advance of travel and engage in more self-service.
- Allow airports and airlines to leverage off the security provided by the DTC in order to enrol a passenger for biometric enabled travel processes.
- Provide aviation stakeholders with advanced passenger authentication well in advance of travel.
- Help support biometric matching that occurs at airport controlled checkpoints, whilst further assisting in improving pre-arrival security and risk assessment.

***How is a DTC secure? Can it be stolen/forged/counterfeited? How is data protected?***

To ensure the same level of security as the current eMRTD, the DTC is based on the hybrid concept of a virtual and physical components linked cryptographically.

The technical specifications behind ePassport issuance offer key attributes that must be maintained in a DTC:

- Verifying entities must be able to authenticate the credentials supplied.
- They should include means to protect against cloning of DTC's.
- They should be capable of accepting and storing pertinent holder and/or travel data.
- They must protect the privacy of the user.
- Verification processes based on these credentials must be as least as secure as for eMRTDs.

The Issuing authority will need to provide security and interoperability requirements for the physical device.

An ePassport allows the legitimate holder to be identified by border officials by employing a combination of physical and digital security features. **In the absence of the physical security features that are provided in a passport book, it is essential that DTC physical authenticators provide the digital security features of active authentication or chip authentication** or any equivalent mechanism.

*Do member states have to issue DTCs?*

No, issuance of DTCs is optional. However, any holder with an ePassport may be able to self-derive a DTC-VC.

*Do member states have to accept DTCs at their border?*

No. This is entirely a decision for each State.

*Can a DTC be used outside of travel?*

Yes, in the same way you could use a passport outside of travel for identification purposes if the other party have the resources to authenticate it.

*Will the DTC be a form of Digital Identity?*

Where verifying authorities can authenticate the DTC, and then it could be used as a form of digital identity.

*Question regarding ETAs Travel history Question re travel stamps and visas, LDS2, ETAs etc.*

While logical data structure 2 (LDS2) does open new possibilities to digitally store this information in ePassports, the first generation DTC will not include functionality to support additional data.

*Can someone have multiple DTCs?*

It is possible for multiple DTC-PCs to be hosted on a single physical device, such as for family groups. However, if this option is exercised, then all potential exploitations of vulnerable groups (e.g. children, etc.) should be carefully considered.

It is possible for multiple DTC-PCs to be hosted on a single physical device where the holder has more than one ePassport (standard and diplomatic, Dual-National, additional etc.)

It is not possible to have multiple DTC-PCs for one issued ePassport.

*How long does a DTC remain valid?*

Where the DTC has its own unique characteristics and identifier (Type 2 & 3), it will include the validity period and validity dates, this is dependent on the individual and the issuing authority within the ICAO Doc 9303 standards. Like a regular travel document, issuing authorities can invalidate a DTC by reporting it to the appropriate domestic and international authorities, when a DTC is lost, stolen, revoked or cancelled it will no longer be valid for travel.

| |
|---|
| *What if I lose it? Is it still valid?* |
| Like a regular travel document DTC can be invalidated by reporting it to the appropriate domestic and international authorities. DTCs that are lost, stolen, revoked or cancelled are no longer valid for travel.<br>Issuing authorities can invalidate a DTC by reporting the issued eMRTD (which has been derived from a record) lost, stolen, revoked or cancelled. The invalidation of the source authorization would automatically invalidate all DTC-VCs linked to that eMRTD.<br>eMRTD bound (Type 1) or eMRTD-PC bound (Type 2) DTCs share the Document Number with an existing eMRTD. Thus, revocation of the existing eMRTD also revokes the DTC. PC bound DTCs (Type 3) do not share the document number with any eMRTD, thus, the PC bound DTC must be revoked on its own. |
| *Will there be different DTC types (Diplomatic, Standard etc)* |
| This would be possible (in the same way you could have multiple physical passports). However, the option to have different types of DTC's is overall dependent on the issuing authority. |
| *Will the DTC have a unique number?* |
| Any DTC that has a physical component other than an eMRTD will have a unique identifier to link the specific VC to the specific PC in a one-to-one association.<br>The eMRTD Bound DTC (Type 1) will not have a unique number specified, as it is made up of a DTC-VC derived directly from the eMRTD (or corresponding authority data) and does not have any other additional physical components.<br>eMRTD PC Bound and PC Bound DTCs (Type 2 and 3) will have unique identifiers to enable a one-to-one association between the VC and the PC. This also enables the reporting of a lost PC.<br>In the case of eMRTD PC Bound (Type 2), the unique identifier is in addition to the Document Number of the associated eMRTD. This enables a PC to be reported lost without the need to invalidate the underlying eMRTD. This will only invalidate the DTC-VC and the associated PC.<br>In the case of PC Bound DTC (Type 3), there is no underlying eMRTD. The Document Number and the Unique Identifier will be identical. Reporting this identifier will result in the invalidation of the DTC. |
| *Does it require specialist equipment?* |
| This is dependent on the implementation strategy chosen by the issuing or verifying authorities. |
| *Can I hold someone else's DTC? Can I have multiple DTCs for my family in one device?* |
| Yes, with different private keys one device could be used as the single physical component.<br>If there are multiple private keys in the same device they don't need to have different access control credentials.<br>It is possible for multiple DTC-PCs to be hosted on a single physical device. (i.e. a parent having a child's DTC on his/her phone). However, if this option is exercised, then all potential exploitations of vulnerable groups (e.g. children, etc.) should be carefully considered. |
| |

# GLOSSARY

| | |
|---|---|
| Access control | To protect the privacy of the travel document holder, data on the chips of ePassports are generally protected by an access control mechanism. These access control mechanisms prevent skimming of the chip data and eavesdropping of the communications between an ePassport and the inspection system. |
| Advanced Passenger Information (API) | Passenger information generated via check in before the arrival of the passenger in the country of destination, to enable relevant border agencies to perform risk-based targeted controls on passengers and the goods they are carrying. |
| 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 | The process of validating the authenticity and integrity of an ePassport by verifying the digital signature on the chip. |
| Authenticators | Physical components that can authenticated, i.e. ePassport, DTC-PC. |
| Automatic Border Control (ABC) | Automated immigration control system where the inspection system of authentication and biometric verification are automated in a 'self-service' model. |
| Basic Access Control (BAC) | First generation access control where the inspection system derives the access key by reading the Machine Readable Zone (MRZ) on the data page of the ePassport . The keys used in BAC are symmetric. |
| 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 a enrolee. |
| 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 verification | 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. |
| Brute-force attack | Trying every possible key and checking whether the resulting plain text is meaningful. |
| Certificate Revocation List (CRL) | A list of revoked certificates within a given infrastructure. |
| Cloning | Creating an exact digital representation/copy of an existing document. |
| Contactless integrated circuit | A semi-conductor device that communicates with a reader using radio frequency energy. |
| Cryptographic device | A device that allows access to information through cryptography. |
| 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. |
| Deriving Entity | An entity the creates a DTC-VC from an existing ePassport. |
| 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. |
| Digital Travel Credential (DTC) | Travel credentials in a digital format that is meant to temporarily or permanently substitute a conventional passport by a digital representation of the traveller's identity. |

| | |
|---|---|
| Document signer | 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. |
| DTC Physical Component (DTC-PC) | The physical component of a DTC that is cryptographically linked to the virtual component. |
| DTC Virtual Component (DTC-VC) | The virtual component of a DTC containing the digital representation of the holder's identity. |
| electronic Machine Readable Travel Document (eMRTD) | An MRTD (passport, visa or card) that has a contactless integrated circuit embedded in it, the capability of being used for biometric identification of the holder and conforming with the specifications contained in Doc 9303 (commonly referred to as an ePassport). |
| Emergency Travel Document (ETD) | Travel Documents issued by Issuing Authorities in situations where it is not possible to issue a standard passport. |
| Extended Access Control (EAC) | Access control to read sensitive biometric data (fingerprint or iris) on the chip of the ePassport. A more complex cryptographic infrastructure than is found in BAC/SAC and also implies an additional Public Key Infrastructure. |
| Facial Recognition Technology (FR) | The process of using an algorithm that compares templates derived from the facial reference (photo) and from the live biometric input (face of holder), resulting in a determination of match or no match. |
| FIDO Alliance (Fast Identity Online) | FIDO authentication standards body for open and scalable standards that enable simpler and more secure user authentication experiences across many websites and mobile services. |
| 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 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, including the development and maintenance of MRTD standards and specifications and provide Member States with a platform to collaborate with industry on the development of international civil aviation Standards and Recommended Practices (SARPs) and policies. The ICAO Traveller Identification Program (TRIP) develops, maintains and promotes international travel document specifications, standards and recommended practices. |
| Integrated circuit | A set of electronic circuits on one small flat piece (or "chip") of semiconductor material designed to perform processing and/or memory functions. |
| International Civil Aviation Authority (ICAO) | A UN specialized agency, established by States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention). |
| International Organisation for Standardisation (ISO) | The International Organisation for Standardisation is an international standard-setting body composed of representatives from various national standards organizations. ISO promotes worldwide proprietary, industrial and commercial standards. |
| 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.<br>The Travel Document Issuing Authority issues the ePassport from which eMRTD Bound and eMRTD PC-Bound 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 a DTC must be issued by a Travel Document Issuing Authority. |
| LDS2 | Second generation of the logical data structure. |

| | |
|---|---|
| Logical Data Structure (LDS) | Describes how data are stored and formatted in the contactless IC of an eMRTD. |
| Machine Readable Travel Document (MRTD) | Official document, conforming to the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel 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. |
| Member states/contracting states | All countries that are affiliated with ICAO and comply with ICAO standards. |
| Passenger Name Record (PNR) | Passenger Name Record data is generated during the booking or buying of an air ticket. |
| Passive authentication | the process of authenticating the digital signature to confirm that the information stored on the chip was saved by the proper authority (i.e. the issuing State) and has not been tampered with. |
| Password Authenticated Connection Establishment (PACE) | Access control, the process for PACE is the same as for BAC; however, PACE employs asymmetric cryptography to establish stronger protection against eavesdropping. |
| Private key | A cryptographic key known only to the user, employed in public key cryptography in decrypting or signing information. |
| Public key | The public component of an integrated asymmetric key pair, used in encrypting or verifying information. |
| 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. Document. |
| Public key infrastructure | 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 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. |
| Supplemental Access Control (SAC) | Used to describe ePassports that have both BAC and PACE. Having both access control mechanisms on the chip, rather than only the newer PACE, ensures that inspection systems at border control can read the chip of the ePassport—this is often referred to as backwards compatibility. |
| Symmetric keys | The same key is used to encrypt the data for transmission to the reader as is used by the reader to decrypt the data. |
| Token | A physical/digital representation of something/someone. |
| Trust Anchor | In cryptographic systems with hierarchical structure this is an authoritative entity for which trust is assumed and not derived. |

**— END —**