ICAO

MACHINE READABLE TRAVEL DOCUMENTS GUIDANCE DOCUMENT

GUIDING CORE PRINCIPLES FOR THE DEVELOPMENT OF DIGITAL TRAVEL CREDENTIAL (DTC)

Version – 5.0 | October 2025

ICAO TECHNICAL ADVISORY GROUP ON THE TRAVELLER IDENTIFICATION PROGRAMME (TAG/TRIP), SUBGROUP OF THE NEW TECHNOLOGIES WORKING GROUP (NTWG)

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

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 travel document, which can in turn be validated using the travel document issuing authority’s public key infrastructure. DTC development is currently focussed on the following travel continuum use-cases: border control, boarding, visa and Digital Travel Authorization (DTA).

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.

   Policy clarification: To ensure confidence in the authenticity and integrity of the DTC, existing eMRTD security mechanisms will be leveraged (passive authentication; anti-cloning; anti-skimming; and access control) and any required alternative protocols must meet existing eMRTD security properties. Methods of validating device security properties will be explored, along with considerations related to securely provisioning the DTC to a device.

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 DTC MUST be backwards compatible with existing inspection systems to ensure minimal changes are required at the border.

   Policy clarification: This principle must be applied to security protocols, but adherence may not be possible in all areas. Any required changes to protocols (e.g., user interfaces, optical readers, contactless readers, etc.) must be clearly outlined, conform with established DTC-VC data and authentication requirements, and be evident to the DTC holder at time of transaction.

6. 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.

7. The revocation of the eMRTD MUST automatically revoke all underlying DTCs.

   Policy clarification: DTC inspection processes should verify the validity of the DTC by assessing the status of the underlying eMRTD.

8. The DTC MUST be issued by a Travel Document Issuing Authority.

   Policy clarification: The DTC's cryptographic link to the issuing authority must remain untouched. Third-party changes or additions to the DTC-VC will impair the security of the DTC and render the credential non-compliant. A DTC may be signed with an additional cryptographic wrapper, but this MUST NOT prohibit or interfere with an entity's ability to read and verify the authenticity of the information using PKI from the issuing authority.

9. The transmission of a DTC MUST be secure and privacy protective.

   Policy clarification: The DTC must be protected during electronic transmission, including the employment of security protocols such as end-to-end encryption, secure endpoint and confirmation of information received.

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. In line with the core purpose of MRTD and eMRTDs, the DTC will continue to provide all traveller identity information required for border processing. In some use cases, a subset of the DTC-VC data content may be derived and sent. This is possible, but it should be noted that it is no longer a DTC but a subset of it (see section 7).

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

   i. The virtual component is an exact copy of the electronic document data, with the exception that DG 3 and DG 4 are not included in the VC data content. See possible exception in section 7.2. The VC contains a link to the physical component
   ii. 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, is unaltered and retains the cryptographic link to the issuing authority
   iii. 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

   i. The physical device serves as the DTC-PC, with the eMRTD as the alternate or as a fallback

   ii. The virtual component is an exact copy of the electronic document data, with the exception that DG 3 and DG 4 are not included in the VC data content. See possible exception in section 7.2. The VC contains a link to the physical component

   iii. The VC may contain additional data at the discretion of the issuing authority

   iv. The DTC-PC MUST host a DTC-VC

   v. For inspection system interfaces, the initial handshake with DTC-PC MUST be as identical as possible to the eMRTD, taking into account technical constraints.

   vi. 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

   i. Only the physical device will serve as the DTC-PC

   ii. The virtual component will use the exact same data elements as defined in the logical data structure of Doc. 9303, with the exception that DG 3 and DG 4 are not included in the VC data content. See possible exception in section 7.2.

   iii. The VC contains a link to the physical component

   iv. The VC may contain additional data at the discretion of the issuing authority

v. The DTC-PC MUST host a DTC-VC

vi. For inspection system interfaces, the initial handshake with DTC-PC MUST be as identical as possible to the eMRTD, taking into account technical constraints.

vii. There SHALL be a distinguishable identifier to recognise the document as a virtual credential without an eMRTD as an alternate or as a fallback

viii. May have its own document characteristics (ID [passport] number, validity period, digital signature, etc).

6. Life Cycle of a DTC

6.1. Creation

DTC creation is optional for States and should not result in burdensome issuance processes for the client.

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 data.

b) Type 2 - eMRTD PC bound (formerly known as 'Authority-Derived DTC'): The DTC-VC is derived from an existing travel document data. 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

The eMRTD-bound (Type 1) DTC will have the same validity as the underlying eMRTD. 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), 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 successfully 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, issuing authorities should only provision one 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 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. Variations

7.1. Variations for Verifiable Data Groups

In some use cases, a subset of the DTC-VC data content may be derived and sent. For example, an airline may prefer or require verifiable data that does not include a biometric. Note that all variations MUST maintain an unbroken and available cryptographic link back to the issuing authority. In practice, this means that the DTC-VC subset used must contain EF.SOD and that individual data groups (DG) cannot be split up. This variation is NOT considered a DTC as it does not contain a biometric and therefore cannot be used to establish identity for the purposes of facilitating border clearance – it is considered a verifiable or 'micro-credential.'

7.2. Variations for Biometrics

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

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 additional access control mechanisms these biometrics could be included in the DTC-VC of the traveller.

7.3. Biometrics and Future DTC Generations

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

8. Transmission Protocols

A DTC-VC is intended to be shared with an immigration crossing point in advance of travel, or for purposes of applying for a Visa or an Electronic Travel Authorization. In these cases, a uniform, interoperable and secure transmission protocol needs to be specified. This section details the requirements that arise from clause 9 of the Guiding Principles. This section does not cover the interface between a DTC-PC and an Inspection System (will be covered in the DTC-PC TR)

The DTC-VC may be located, for example, in an identity wallet on a mobile device or as a file on a laptop computer. The DTC-PC may also be located on the same mobile device. The following principles apply regardless of the location of the DTC-PC or DTC-VC.

1. The holder of the DTC must consent to the transmission of the DTC-VC.
2. The endpoint to which the DTC is submitted must be authenticated and this endpoint must be verifiable by the submitter.
3. The DTC-VC must not be transmitted in an unencrypted form. It must be encrypted specifically for the intended recipient, ensuring that only the authorized endpoint can access the data. Relying solely on TLS encryption at the transport layer is insufficient for this purpose.
4. If the submission to the endpoint happens through intermediaries routing the information to the endpoint, the intermediate entities should not be able to access the DTC-VC information. Additional information that allows the intermediaries to route the DTC-VC to the correct end-point should be part of the transmitted datagram.
5. The transmission protocol shall allow for the transmission of additional information (e.g. flight number, destination, date etc.) to be added to the transmitted datagram.
6. An endpoint response must be sent back to acknowledge receipt of the DTC-VC.
7. The endpoint response may contain information that the DTC holder can additionally provide as supplementary information as part of the protocol or in another manner. The protocol always ends with the response given by the endpoint.
8. If the DTC-VC is in the ID wallet and there is additional information available in another application on the same mobile device, the ID wallet can obtain the necessary information directly from the other application. A standardized interoperable mechanism for retrieving information must be used in communication between applications.
9. The eMRTD trust framework shall be the basis of trust in the transmission.

9. 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 processing, 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.
- Confirm the validity of the underlying eMRTD.

10. 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: 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). 2. The biometric comparision of the biometrics contained in the DTC-VC and the traveler (including verification of authenticity via Passive Authentication) Additionally, the link between DTC-VC and DTC-PC/eMRTD must be checked. 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 traveller	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. This is the same as the issuance of an eMRTD to an unentitled traveller. 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: 1. Requiring in-person enrollment; and/or 2. Requiring a 1-to-1 biometric match [using facial recognition] to support enrollment; and/or 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: 1. Secure communication channel between the smart device and inspection equipment; and/or 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 4. User consent before transmitting the VC 5. Ensuring that travel document holders are aware of and using channels to report compromised DTCs.

The phone holding a DTC-VC is lost or stolen.	If the phone is able to be unlocked and the DTC-VC accessed, criminals could present as the holder for travel or other services.	Yes	As the DTC-VC is a verifiable electronic copy of the data in the passport, which can be cloned and potentially placed on multiple devices, the mitigations involve employing passive authentication and biometric matching to ensure the holder using the document is bona fide. States will need to undertake their own risk assessment regarding the potential for misuse, and whether this presents any additional risk, and take action accordingly. This may include security employed on the device to protect the DTC-VC (e.g. secure wallet or multi-factor authentication). Upon determining the risk, States may decide to invalidate the underlying passport where the risk of misuse is deemed high.
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. 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. However, there is a chance that travellers 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: 1. Communication campaigns to ensure that travellers are aware of the risks associated with holding a DTC-VC on a DTC-PC; and/or 2. Encouraging DTC holders to register their devices to assist in DTC management; and/or 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. 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: 1. Establishing security requirements for the hardware and certification; and/or 2. Communication with DTC holders.
Not reporting Lost/stolen/decommission DTC-PCs	The impact is similar to the loss of and eMRTD	Partially. 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 travellers, 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 travellers 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 inspection system has an outage, there is no fallback to a "physical" document	Yes. For PC-Bound DTC	None
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 traveller could be falsely deemed unable to board a flight or enter a country.	Yes. For PC-Bound DTC	None

11. Other Considerations

11.1. Diplomatic, Official and Other Passports

The use of a standardized second character [in the machine-readable zone] to denote a specific type of passport will become mandatory starting January 1, 2026.

Limited use of the standardized second character in the lead up to the mandatory implementation date, 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 identify the passport/DTC type (regular, diplomatic, etc.) will present 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.

11.2. 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.

11.3. 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.

12. Implementation Plan

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

1. DTC-VC
2. DTC-PC

DTC-VC specification document is complete and endorsed. It can be used to issue eMRTD bound DTCs. Once the DTC-PC is specified and endorsed, specifications can be used to issue all types of DTCs.

— — — — — — — —

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 traveller. Each of these initiatives involves creating a package of verifiable traveller 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 traveller 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 traveller 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 traveller actually arrives in their destination country. The DTC-VC, sent in advance of the traveller 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) 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.

— — — — — — — —

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 an 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 that 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 credential in a digital format that conforms with the specifications contained in ICAO DTC Technical Reports (and once incorporated, in Doc. 9303) and are meant to temporarily or permanently substitute a conventional passport with 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 that has an embedded contactless integrated circuit, 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. 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)	Travel document, conforming to the specifications contained in Doc 9303, 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 (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 —