MACHINE READABLE TRAVEL DOCUMENTS GUIDANCE DOCUMENT

ICAO TRIP GUIDE ON ICAO DIGITAL TRAVEL CREDENTIAL (DTC)

PART 1 - IMPLEMENTATION GUIDANCE FOR STATES

Version – 1.0 | September 2025

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

TABLE OF CONTENTS

1. The ICAO Digital Travel Credential (ICAO DTC)

1.1 *What is a Digital Travel Credential?*

A *digital travel credential* ("DTC") is a secure, globally interoperable *digital companion* and/or *substitution* to a physical electronic machine-readable travel document (eMRTD). The DTC, in temporarily or permanently substituting a conventional passport with a digital representation of a traveler's identity, is intended to support seamless travel.

An ICAO-compliant DTC *must*:

- Have a *virtual* component that 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); and
- Maintain an unaltered cryptographic link to the issuing authority.

  NOTE: Subsets of DTC *virtual* component data contents 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. This type of variation also would NOT be considered a DTC, as it is not an exact copy of the electronic document data – it would be considered a verifiable or 'micro-credential.'

Just as with ICAO-compliant eMRTDs, successful validation of the issuer's cryptographic link (accomplished using the travel document issuing authority's public key infrastructure) enables verifying entities to establish both authenticity and integrity of issuance of the DTC, thereby serving as the most reliable anchor of trust. Altering the ICAO DTC, or resigning individual data elements post-issuance, breaks the intended chain of trust and challenges a verifying entity's ability to establish the authenticity and integrity of the DTC.

ICAO DTC opens opportunities to alter the status quo for traveller information flow. With DTC, authorities can receive, and establish trust in, a digital representation of the passport data *before* a traveller's actual arrival. Key benefits of this change in traveller information flow include:

- For *border authorities,* opportunities to streamline border management and find new process efficiencies (for example, in travel authorization processing, pre-arrival screening and biometrically enabled processes);
- For *travel document holders,* an increasingly seamless point of entry/exit experience when travelling across a border.

Beyond immediate improvements to traveler information flows, as ICAO continues to advance the concept, ICAO DTC may also offer *travel document issuing authorities* opportunities to modernize the ways in which they deliver services to clients.

1.2 ICAO's Approach to Travel Document Specifications Development

ICAO is advancing DTC in alignment with one key principle which also guided electronic machine readable travel document (eMRTD) specifications – *the hybrid approach*.

Electronic MRTDs were developed featuring a combination of 1) a *virtual* component, consisting of the data in the passport's contactless integrated circuit chip ("chip"), and 2) a *physical* component, consisting of the chip within the physical booklet, which is cryptographically linked to the *virtual* component. By uniquely linking the *physical* component to the *virtual* component (for eMRTD - the chip within the physical passport book) via cryptography, issuing authorities can ensure receiving entities can establish an unbroken link back to the proper issuing authority.

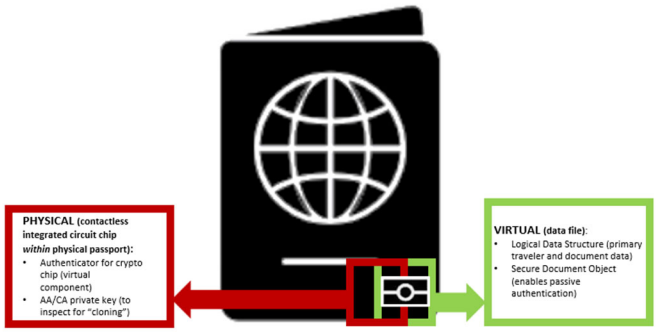

Figure 1 – eMRTD – Physical and Virtual Components

1.3 Development Plan for ICAO DTC

ICAO DTC, in exploring linking the *virtual* component to *new form factors* for *physical* components, would support a gradual reduction in reliance on traditional physical passport books. Because a cryptographic link will continue to be maintained between a *virtual* and *physical* component, verifying entities, when an appropriate mix of checks are undertaken, would continue to be able to confirm copy and access controls as can be done currently, with eMRTD.

> **NOTE**: Besides *passive authentication* and *chip access control,* issuing authorities may choose additional security, using more complex ways of securing the chip and its data.

The ICAO DTC will be implemented in three different ways (outlined visually below). ICAO DTC types are not hierarchical, nor do they represent evolving DTC solutions. Each ICAO DTC implementation "type" is comprised of a DTC-VC and a DTC-PC. Recall that a DTC's *virtual* component is a file that can be stored on any medium and does not have any inherent access protection; however, by *linking* that *virtual* component to a *physical* component, the issuer can provide access control mechanisms for further protection. All DTC implementation types leverage the same technical specifications for the DTC *virtual component* – it is the *physical* component that will evolve, depending on the type of DTC implementation.

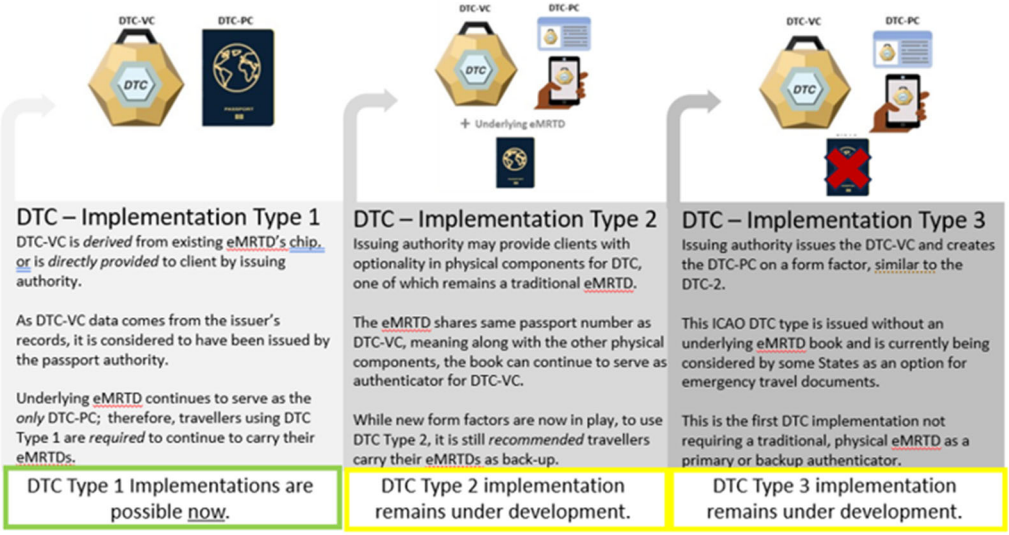

Figure 2 – ICAO DTC Approach – Implementation "Types"

1.4 ICAO's Existing Body of Work on Digital Travel Credentials

ICAO's work on DTC is advancing on several different thematic fronts.

To find quick answers to some of the more common questions that might be asked respecting ICAO DTC, and the resources available to assist in addressing them, please refer to **Annex A**.

1.5 How DTC Fits in ICAO's Progression of Globally Interoperable Travel Document Specifications

ICAO's development of DTC is aligned with the historical progression of other globally interoperable travel documents specified by ICAO, starting with *machine-readable travel documents* (MRTDs), to *electronic machine-readable travel documents* (eMRTD), through to the present (DTC).

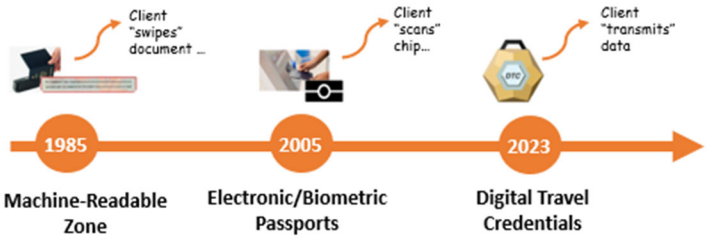

Figure 3 – Timeline – Evolution of ICAO-Compliant Passport

2. About this Guidance – Scope and Application

This Guidance complements the existing endorsed ICAO policy, technical and guidance pieces advancing DTC (as outlined in **Annex A**) by highlighting to Member States key implementation considerations that will help them situate DTC in their existing, or future, domestic traveller identification and processing ecosystems.

This Guidance also aims to generate State thinking around appropriate business requirements for DTC implementation, as well as options for sequencing of key components, taking into considering unique national circumstances.

2.1 FOCUS - ICAO DTC *Type 1* Implementation

As outlined above, ICAO's approach to DTC development involves three implementation "types".

This Guidance will focus on DTC Type 1 implementation ("DTC-1"). DTC-1 implementations are enabled by ICAO-endorsed technical specifications for a DTC *virtual component* (referenced in **Annex A**). In this implementation, the DTC's *physical* component remains the already issued eMRTD. As the generation of the DTC's *virtual component* uses issuing authorities' existing records, or an already-issued eMRTD, DTC-1 implementations are possible now.

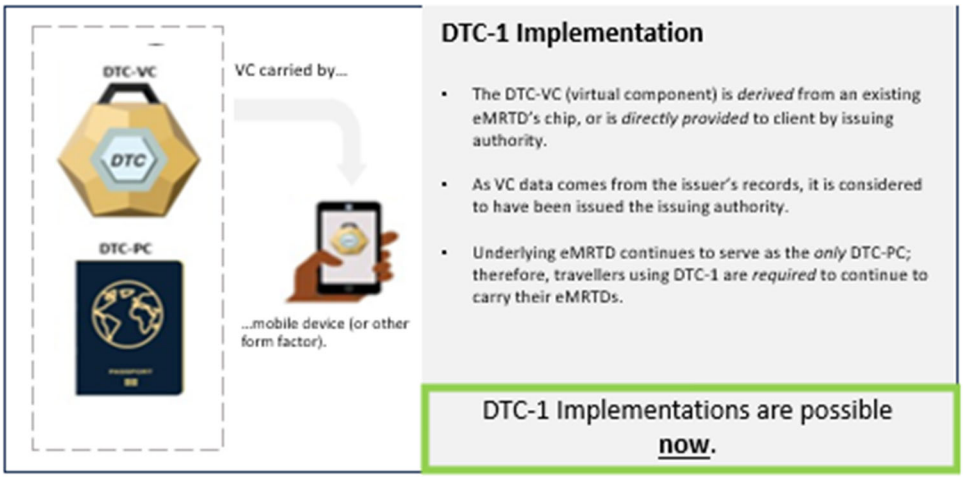

Figure 4 – ICAO DTC Approach – Type 1 Implementation

2.2 Intended Audience

Given the nature of DTC Type 1 implementations, primary considerations relate to the use of passport data that has already been authoritatively issued. The Guidance is targeted to stakeholders on the use side of travel document information, with a particular focus on border entities.

While primary considerations for DTC-1 relate to post-issuance use of passport data, as DTC Types 2 and 3 are advanced, the considerations will broaden to include more upstream elements of the traveller identification continuum, including issuance. Therefore, this Guidance

may also be useful for the full range of stakeholders involved in traveller identification, including authoritative issuers.

2.3 ICAO DTC and Border Control

As with a traditional travel document, a DTC is just one component of a State's broader border control management approach. This Guidance on DTC-1 implementations aims to extend some already existing ICAO resources aimed at supporting State planning for border control management which focus on use of machine-readable and electronic machine-readable travel documents in border control systems. These existing resources include the *ICAO TRIP Guide on Border Control Management* and the *ICAO Automated Border Control (ABC) Cost Benefit Analysis Tool*. Both resources are referenced in **Annex A**.

This Guidance acknowledges that ICAO Member State border control arrangements vary greatly throughout the world. States with more mature arrangements may have capabilities in place relating to accessing, reading and leveraging the data from an ICAO Doc 9303-compliant ePassport using automated border control, at points of entry. These types of automated document inspection processes enable States to verify traveller document data more quickly and with a higher level of confidence; States with these kinds of inspection capabilities are particularly well-positioned to implement DTC-1.

2.3 ICAO DTC and Other Digital Credentials

ICAO, while remaining focused on meeting the requirements for the primary cross-border travel use case, recognizes that ICAO DTC exists in an increasingly complex and evolving ecosystems of "digital credentials". These other ecosystems and credentials are intended to address a variety of use cases, with different levels of identity assurance. This complex environment presents both challenges and opportunities for ICAO Member States considering DTC implementation.

Respecting travel, for example, airlines require subsets of passport data verifiable online to enhance customer experience by moving checks off airport in advance of travel. The International Air Transport Association (IATA) has addressed this need via its ***One ID*** concept, which defines a process and a standard for creating a digital copy of the passport. This process can be anchored, when available, on an ICAO-specified eMRTD or ICAO DTC (and the underlying trust architecture for these credentials already established by ICAO), serving as an early example of how ICAO DTC can support, or even enhance, solutions intended to address non-border-related use cases.

Given ICAO Member States will individually determine acceptability of not just ICAO DTC, but also other digital credentials for a variety of purposes, it is highly beneficial for those considering DTC implementation to be aware of other digital credential initiatives underway in domestic or regional contexts. This could be achieved via engagement between entities responsible for travel document issuance and those in charge of broader digital credential initiatives (for example - other electronic identification schemes).

2.4 ICAO DTC – Member State Standards and Recommended Practices

> **NOTE**: Just as is the case with eMRTD, issuance of, and acceptability at borders of, ICAO DTC remains optional for Member States – it is not an obligation. ICAO is advancing the global model for DTC, as well as the technical specifications and operational guidance to support States with implementation - but individual Member States ultimately can decide for themselves whether DTC is a good option, depending on their own unique circumstances.

Standards and Recommended Practices - ICAO's Annex 9

As yet, there are no Annex 9 *Standards* or *Recommended Practices* specific to issuance of, or use of, DTC. Given DTC is being developed in alignment with the issuing and verification architecture that already exists for eMRTD, there is, however, a framework applying to use of *automated tools* to validate eMRTDs (for example, including, but not exclusively, *automated border control*) by border authorities that provides insights into future DTC use. Such existing *Standards* and *Recommended Practices* may be considered as intermediary for States considering of Type 1 DTC implementations.

For example, Annex 9 contains the following *Recommended Practices* for Member States relating to the ability to leverage eMRTD verifications:

RELEVANT ICAO STANDARDS AND RECOMMENDED PRACTICES

Extract from ICAO Annex 9 – *Facilitation*, Chapter 3 – Entry and departure of persons and their baggage[70]:

H. Inspection of Travel Documents

"…

3.37 **Recommended Practice.—** *Contracting States implementing checks on eMRTDs at border controls should join the ICAO PKD and use the information available from the PKD to validate eMRTDs at border controls.*

3.38 – **Recommended Practice**. – *Each Contracting State should, as far as practicable, query, at entry and departure border control points, the travel documents of individuals travelling internationally against INTERPOL's SLTD database.*

3.39 **Recommended Practice. -** *Each Contracting State should consider the introduction of Automated Border Control (ABC) systems in order to facilitate and expedite the clearance of persons entering or departing by air.*

3.39.1 **Recommended Practice.—***Contracting States utilizing ABC systems should, pursuant to 3.15 and 3.39, use the information available in the PKD to validate eMRTDs, perform biometric matching to establish that the passenger is the rightful holder of the document, and query INTERPOL Stolen and Lost Travel Documents (SLTD) database, as well as other border control records to determine eligibility for border crossing.*

3.39.2 **Recommended Practice.—***Contracting States utilizing ABC systems should ensure that gates are adequately staffed while operational to ensure a smooth passenger flow and respond rapidly to safety and integrity of a system malfunction…"*

Technical Specifications - ICAO's Doc 9303 for Machine-Readable Travel Documents

ICAO's Doc 9303 for Machine-Readable Travel Documents, which lays out technical specifications for travel documents (with particular application to the passport), also references security mechanisms, some of which are considered mandatory (for example, passive authentication), for Member States that are both issuing and leveraging eMRTDs at borders:

RELEVANT ICAO TECHNICAL SPECIFICATIONS

Extract from ICAO's Doc 9303 for *Machine-Readable Travel Documents*, Part 11, *Security Mechanisms for MRTDs*

"...

(**Section 3 – Securing Electronic Data**): *Besides Passive Authentication by digital signatures and Chip Access Control, issuing States or organizations MAY choose additional security, using more complex ways of securing the contactless IC and its data.*

(**Section 4 – Access to the Contactless IC**): 4.4.3.5.2 – "*Note.— Passive Authentication MUST be performed in combination with the Chip Authentication Mapping. Only after a successful validation of the respective Security Object may the eMRTD chip be considered genuine...*"

3. A TRAVELLER INFORMATION FLOW INTEGRATING ICAO DTC – FOUNDATIONAL CONSIDERATIONS

(NOT YET DEVELOPED - FOR PHASE 2/TAG-TRIP6)

- Operational Policy
- Legislation/Regulations
- Privacy and Use of Personal Information
- Technical Requirements and Capacity
- Key Stakeholders – the Consortium
- Change Management
- The User Experience

4. A Traveller Information Flow Integrating ICAO DTC (DTC-1)

4.1 Generating a DTC by *Derivation* (DTC-1)

CONSIDERATIONS:

- ✓ DTC-1 involves a DTC *virtual* component (DTC-VC) being generated by *deriving* data from an existing ICAO Doc 9303 compliant ePassport's chip.
- ✓ While the DTC-VC can be carried on many mediums following derivation, for DTC-1, the authoritative *physical* component remains the already-issued ePassport; any other mediums are *carriers only*.
- ✓ The act of generating a DTC via *derivation*, which can be initiated by the document holder or other third party, is unique to DTC-1 implementations.
- ✓ Because a Type 1 DTC is *derived* from a Travel Document Issuing Authority's data, it is considered to have been *issued* by that Authority.
- ✓ Where interoperable with other national systems and databases, enabling *derivation of* a DTC is a critical first step to position States to receive passport data *in advance* of a traveler's arrival.

4.1.1 <u>OVERVIEW</u>

For a DTC-1 implementation, the means of generating the DTC *Virtual Component* ("DTC-VC") is *derivation* from an existing, already-issued electronic passport chip, or a travel document issuing authority's existing record. The DTC-VC data can then be stored on a medium other than the originating eMRTD, for example a mobile device. However, for DTC-1, those other mediums are <u>not</u> authoritative containers for DTC-VC data – the originating eMRTD remains the DTC's *physical* component. Therefore, travellers using a DTC-1 are still required to travel with their physical passports.

> **<u>NOTE:</u>** An ICAO-compliant DTC *Virtual Component* ("DTC-VC") is an *<u>exact copy</u> <u>of all the data</u> contained on an eMRTD's chip*, with the exception that DG 3 and

DG 4, given these data elements are *secured by additional mechanisms* upon issuance. The DTC-VC must also include the *secure document object* ("SOD") data from an eMRTD's chip, as this data is required to rebuild the data's cryptographic link back to the issuing authority.

The act of generating a DTC-VC by *Derivation*, including the direct involvement of document holders in initiating this action (or with the help of third parties), is unique to the DTC-1 implementation.

Just as with automated border control systems, States can also integrate different types of security mechanisms and verifications in a derivation step. Consideration of these additional layers of checks could mean additional technical requirements, and provision of additional guidance to support clients to ensure they can successfully complete all steps.

> **NOTE:** The same security mechanisms that already exist for eMRTD can also be leveraged by Member States for verification of a DTC-VC, as means of establishing trust in the data. For example, as with an eMRTD, performing *passive authentication* of a DTC-VC proves that the contents of the DTC-VC are *authentic* and *unchanged* since point of issuance. *More on these security mechanisms can be found in Section 4.4 - DTC Verification.*

This section will focus on the core elements of a DTC-VC generation by *derivation* step – that is, supporting clients in accessing their existing ePassport chip data.

4.1.2 *Operationalizing the DTC Type 1 Generation (by Derivation) Step*

The generation (by derivation) step replicates some of the steps that many States have already operationalized via processes aimed at enabling automatic verification of ePassport chip data via, for example, automated kiosks. However, DTC-1 envisions pushing some steps off airport, and in more direct control of document holders - resulting in a different data flow, with potentially different technical requirements and new backend connections required, and with an increased level of direct client engagement in the process.

Direct involvement of document holders in this step means States should consider the right capacities (for example, a mobile application on a device) and guidance to enable clients to successfully initiate and complete the action of derivation by directly accessing the data on their own ePassport chips. Alternatively, States could consider means of allowing document holders to request transmission of this data via other means supported by authoritative passport issuers.

States may consider several non-exclusive options for *Derivation*, including, but not limited to:

i. Self-Derivation: allow individuals to create the DTC by using an NFC-enabled device and application to scan the eMRTD; and
ii. Assisted Derivation: allow individuals to request from their national authorities a DTC based on their existing eMRTD.

Self-Derivation

The act of accessing data on an ePassport's chip is open-source (i.e. non-proprietary), and involves two steps – an *optical character recognition* step where an ePassport's *machine-readable zone* is read via automated means, enabling by either *basic access control* ("BAC") or *password authenticated connection establishment* ("PACE"), where access to the data on the ePassport's chip is granted. The second step is *near-field communication,* where the chip can be accessed by a reader, making the data available to read out[1]. More on these access mechanisms can be found in the *PKD validation roadmap*, referenced in **Annex A.**

This act off accessing and extracting ePassport data is already occurring on a regular basis at many airports throughout the world, enabled by properly configured automated border control systems, which can also be configured to perform the necessary additional checks to establish trustworthiness of that data.

DTC-1 envisions *mobile applications* being deployed to allow individuals to access the chip of their ePassport and derive a DTC using mobile devices. As observed in early DTC implementations, the combination of certain mobile devices and certain ePassports may lead to a variety of new challenges relating to the actual derivation process that merit consideration by Member States - including, for example, the NFC capabilities of the device and the type and location of the antenna in the ePassport[2].

> **NOTE:** Particularly in the early stages of global rollout, it is beneficial for *authoritative issuers* to be aware of, and even actively input on (in support of *border authorities'* risk assessments), methods of *self-derivation* for DTC Type 1.

States may also choose to deploy *kiosk-like devices* at various locations to enable individuals to self-derive their DTC without having NFC-capable mobile devices at their disposal.

Assisted Derivation

Assisted derivation solutions could also be implemented by States in a variety of different ways. States could e.g. allow individuals who apply for a new electronic passport to request the issuing authority to create a DTC alongside issuing the physical ePassport and transmit it to the applicant. While this may impose additional costs to issuing authorities, they should be limited since States or their service-providers responsible for manufacturing ePassports and personalising the chips are already in possession of all the necessary data, software and hardware for generating a DTC.

[1] Note that accessing an ePassport chip's primary data does not automatically infer trustworthiness of that data – ICAO recommends *passive authentication* of passport chip data before relying on that data for transactions requiring a high level of confidence.
[2] DTC1 pilot in The Netherlands Final evaluation report | Rapport | Rijksoverheid.nl p 28

Additionally, States with comprehensive national ePassport registries that contain all the necessary data elements (as prescribed in the TR) could allow individuals to remotely request a DTC based on their existing ePassport.

Assisted derivation solutions, when implemented with "live enrolment" i.e. the person arriving physically at the location of the authority, have the benefit of increased security and accessibility/inclusivity, although they are less user-friendly in the sense that they require physical appearance.

4.1.3 EARLY IMPLEMENTATIONS - MODELS

As demonstrated by early implementations of DTC-1, each State needs to consider its own unique desired outcomes for the DTC creation by derivation step, which in turn will assist in determining the appropriate capacities required to achieve those outcomes.

DTC Type 1 implementations thus far have focussed on supporting clients themselves in deriving a DTC. While sharing the same desired outcome, different approaches have been taken with respect to the level of authority oversight for the derivation step.

It should be noted that early implementations of DTC-1 have been characterized by tight eligibility requirements, and one-way, rather than return, traveller journeys. Early implementations have also featured DTC-VCs which have been *pre-validated* and *linked to the traveller* via biometric checks at point of derivation before submission, as well as being *linked to a specific journey* (via eligibility).

Considerations for DTC-1 *Creation* by *Derivation* Step:

Desired Outcomes:	**Capacities:**
Country A • Client able to derive DTC-VC in an *uncontrolled* environment (off airport)	**Existing:** • Experience performing ePassport verification (passive authentication and other related checks), biometrics/facial matching at points of entry
	New for DTC-1: • Development of native mobile application capable of enabling clients to import DTC-VC themselves (and made available for download)
Country B • Client able to derive DTC-VC in a *controlled* environment (on airport)	**Existing:** • Experience performing ePassport verification (passive authentication and other related checks), biometrics/facial matching at points of entry
	New for DTC-1: • Development of *digital identity wallet* with ability to receive derived DTC-VC (and made available to clients for download) • *Authority-controlled kiosk* to manage actual DTC-VC derivation, transmit encrypted DTC-VC to client's wallet

4.1.4 *EARLY IMPLEMENTATIONS – LEARNINGS*

Early observations from DTC-1 implementations have revealed some key issues to be addressed as the DTC concept, and its supporting technologies, are advanced and as implementations are expanded to more clients and more journey scenarios (i.e. round-trip journeys).

Desired Outcomes:	Early Observations and Learnings:
Country A • Client able to derive DTC-VC in an *uncontrolled* environment (off airport)	• Clients experienced challenges in completing their own DTC derivations. • Tracked statistics pointed to both 1) technical limitations at the time of implementation, and 2) a steep learning curve for clients in navigating their ePassports/mobile phones, as challenges. • The solution was still generally regarded as positive; feedback also indicated the challenges were not seen by clients as blocking them from participating. • Improvements in the user experience were also seen to be possible going forward.
Country B • Client able to derive DTC-VC in a *controlled* environment (on airport)	• More controlled derivation scenario eliminated **some**, but **not all**, of the design-based challenges with the supporting mobile application observed by Country A.

The level of control and oversight in these early implementations is likely to require re-examination in situations where expanded eligibility is sought, and where scenarios involve round-trips or transit, where multiple border inspection entities could be involved in traveller journeys, or perhaps no imminent journey at all.

4.2. Storage

(NOT YET DEVELOPED - FOR PHASE 2/TAG-TRIP6)

4.3. Transmission

(PLACEHOLDER - FOR PHASE 2/TAG-TRIP6)

4.4. Verification

(NOT YET DEVELOPED - FOR PHASE 2/TAG-TRIP6)

4.5. Revocation

(NOT YET DEVELOPED - FOR PHASE 2/TAG-TRIP6)

5. CONCLUSIONS

(NOT YET DEVELOPED - FOR PHASE 2/TAG-TRIP6)

ANNEX A

ICAO DTC Questions and Answers (and Key Resources)

Question	Quick Answer	Reference
What is the **policy basis** on which ICAO is advancing development of DTC?	Subject matter experts from ICAO Member States have articulated a set of guiding policy principles intended to frame the advancement of technical work required to implement the ICAO DTC.	*Guiding Core Principles for the Development of Digital Travel Credentials (DTC)*
What is an ICAO-compliant DTC, from a **purely technical standpoint**?	Guided by ICAO's foundational policy work, subject matter experts have been advancing technical specifications required by Member States seeking to implement DTC.	*Technical Report - ICAO DTC Virtual Component* *Technical Report - ICAO DTC Physical Component*
How can I **encourage a better understanding of the technical underpinnings** of ICAO DTC?	Guided by ICAO's foundational policy work, subject matter experts have been advancing technical specifications required by Member States seeking to implement DTC.	*Technical Report - ICAO DTC Virtual Component* *Technical Report - ICAO DTC Physical Component*
How can I **initiate the conversation** amongst the various stakeholders involved in traveller identification in my State around ICAO DTC, or simply better guide ICAO DTC-related conversations?	ICAO subject matter experts have developed a product aimed at supporting Member States' efforts to explain the ICAO DTC concept to non-technical audiences domestically.	*High Level Guidance: Explaining the ICAO Digital Travel Credentials*
What are my State's **obligations** relating to ICAO DTC?	There are currently no standards for use of DTC by ICAO Member States. DTC use is not an ICAO obligation – it is fully *optional*.	*Existing ICAO Member State obligations are articulated in Annex 9.*
What are **the recommended practices** for my State relating to ICAO DTC?	There are currently no recommended practices relating to DTC for ICAO Member States.	*Existing ICAO Member State recommended practices are articulated in Annex 9.* *From Annex 9, 16th edition:* *3.33.4* Recommended Practice.— *Each Contracting State should consider the introduction of Automated Border*

	Verification of DTC, however, is not overly different from verification of electronic passport, where there *are* existing recommended practices.	*Control (ABC) systems in order to facilitate and expedite the clearance of persons entering or departing by air.* *3.33.5* Recommended Practice.— *Contracting States utilizing ABC systems should, pursuant to 3.9.2 and 3.10.1, use the information available from the PKD to validate eMRTDs, perform biometric matching to establish that the passenger is the rightful holder of the document, and query INTERPOL's Stolen and Lost Travel Documents (SLTD) database, as well as other border control records, to determine eligibility for border crossing.* *3.33.6* Recommended Practice.— *Contracting States utilizing ABC systems should ensure that gates are adequately staffed while operational to ensure a smooth passenger flow and respond rapidly to safety and integrity concerns in the event of a system malfunction.* *ICAO's Doc 9303 Part 11 – Security Mechanisms for MRTDs also notes the passive authentication* (PA) *security mechanism is considered* ***mandatory*** *from a technical specifications perspective, for both issuance and verification of an eMRTD's electronic data.*
How can I ensure my State's border authority is aware of the range of **possible checks for electronic passport**, and for **ICAO DTC**, to establish higher levels if assurance in the document at points of entry?	A technical description of how to access an eMRTD's chip data, as well as the mandatory and optional security mechanisms enabling establishment of trust in the data, can be found in **ICAO's Doc 9303 for Machine-Readable Travel Documents** – specifically **Part 11, *Security Mechanisms of MRTDs*.** A more flow-based overview of the checks available to border authorities when inspecting electronic passports, including the recommended practice of *passive authentication* to establish trustworthiness of data extracted from ePassport chips, can be found on the ICAO Public Key Directory website – the **Electronic Passport Validation Tool**.	ICAO Doc 9303 - Part 11 - Security Mechanisms for MRTDs *Electronic Passport Validation Roadmap Tool*

	Many, if not most, of these checks can be extended to the ICAO DTC.	
My State is considering implementation of **automated border control**/expansion of existing automated border control. Does ICAO have any resources to assist with this?	Yes – ICAO has **cost-benefit analysis tool** associated with exploration of *automated border controls* intended to support more informed Member State decision-making around these controls.	ICAO PKD - ABC Cost Benefit Analysis
Where can I learn more about the existing **real-world implementations** of DTC-1?	The European Commission is actively piloting the DTC in the Schengen area, and those European States involved have provided **reporting** on their DTC-1 experiences and observations.	DTC1 pilot in The Netherlands Final evaluation report | Rapport | Rijksoverheid.nl EUR-Lex - 52024SC0671 - EN - EUR-Lex

— END —