SciencesPo

TECH & GLOBAL AFFAIRS
INNOVATION HUB

DIGITAL TRAVEL CREDENTIALS

Removing Turbulence in Air Travel Identification

Laurent GROSCLAUDE
Assistant Professor, University Toulouse Capitole

Gaetan PRADEL
Cybersecurity Specialist, INCERT

Laurent GROSCLAUDE is an Assistant Professor of business and aviation law at the University of Toulouse Capitole. He holds a PhD from the Paris Sorbonne University in corporate law. He runs the LL.M. International Aviation Law and is guest lecturer at ENAC, ISAE-Supaero and foreign Universities mostly in Asia-Pacific. Laurent publishes papers in international corporate law, aviation law and trade compliance.

Gaetan PRADEL is a cybersecurity specialist at INCERT, a public agency from Luxembourg, specialized in applied cryptography and standardization for ID management. Holder of a PhD in cryptography from Royal Holloway, University of London, Gaetan represents Luxembourg in international standardization organizations such as the ICAO, ISO and IATA. As an editor of multiple cryptography-related standards, Gaetan has contributed to encryption algorithms, random bit generation, and more recently post-quantum digital signatures.

The authors are grateful for the editorial contributions and thoughtful feedback from **Pierre Noro**, Advisor of the Tech & Global Affairs Innovation Hub, whose support greatly enhanced the elaboration of this policy brief.

This document is part of the Policy Brief series published by the Paris School of International Affairs (PSIA) Technology and Global Affairs Innovation Hub.

The Hub's core mission is to accelerate collaborative technology and international governance to address global challenges. Its activities are specifically focused on technology and democracy, defense and security, sustainability and prosperity.

Learn more about the Hub on our website: www.sciencespo.fr/psia-innovation-hub/

Published in April 2025.

Suggested citation: Grosclaude, Laurent & Pradel, Gaetan, *Digital Travel Credentials*, policy brief commissioned by the Paris School of International Affairs Tech & Global Affairs Innovation Hub, April 2025.

INTRODUCTION

The emergence of the digital travel credential (DTC) as an innovative system aiming at facilitating air travel experience and borders crossing takes place in a context of booming of passenger's flow and rise of serious security concerns (1) ; DTCs could have multiple and promising application and relies on elaborated cryptographic techniques (2) ; DTC implementation has already been experimented at a reduced scale and requires a modification of the current legislative framework (3) ; this new technique raises diverse challenges and is confronted to significant current brakes (4) ; and a set of recommendations will conclude this brief paper.

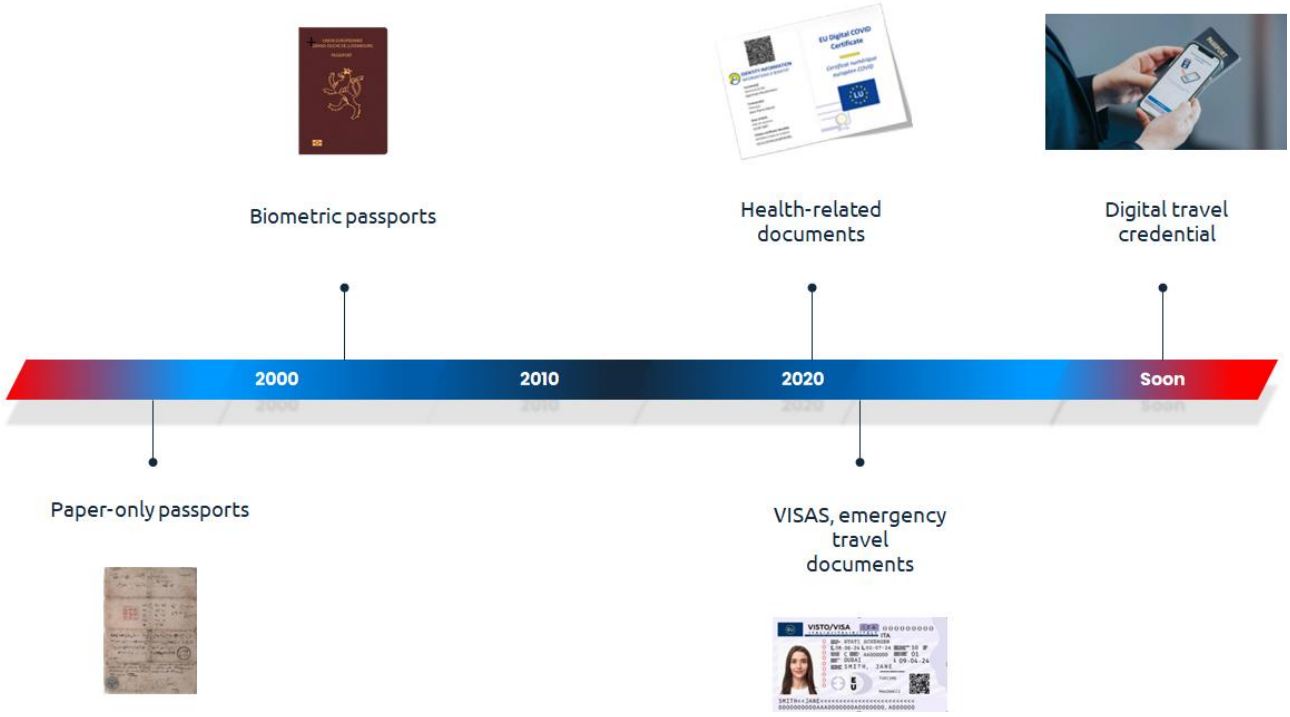
1. CONTEXT

Digitalization has gradually made its way into passenger air transport and borders crossing. Back in the 90's, air transport was all about ink and paper: tickets, passports, visa applications and issuance, immigration and customs check… Machine readable passports appeared in the 1980s, based on an optical data reading (machine readable zone made of 2 lines and 44 characters). Then came biometric passports, booklets with an embedded microprocessor chip containing biographic (e.g. date of birth, surname…) and biometric information (e.g. eye color, fingerprints…).

Malaysia first e-passport, as indicated by the "chip inside" symbol under the "Passport"

Malaysia was the first country to issue biometric passports in 1998. However, the biometric passport as we know it today, i.e. "e-passport" or eMRTD (for electronic Machine-Readable Travel Document), compliant with the International Civil Aviation Organization (ICAO) specifications[1] was firstly issued by Belgium in 2004. Nowadays, over 170 countries issue e-passports to their citizens. In modern airports, eMRTDs may be used in conjunction with standardized biometric identification systems such as facial, iris and/or fingerprint recognition to authenticate travelers. These eMRTDs are increasingly integrated with other systems developed in parallel, such as e-ticketing standards implemented by the International Air Transport Association (IATA) since 1997, and electronic visa processing and electronic travel authorization deployed by States (first ETA launched in 1996 in Australia / 2008 for the US ESTA).

Initiated by the ICAO, the DTC system, as described below, is a key step towards the full digitalization of borders crossing and airport facilitation, defined as an efficient and secure management of the flow of passengers and goods through airport facilities. The DTC is set to offer substantial efficiency gains and economies of scale, in a context of rising competition, both between transportation modes–e.g. between rail and air transport–and within the aviation sector, airport platforms and airlines racing to attract passengers.



From physical to digital: the shift in travel identification documents

Air transport in 2025 is undoubtedly at a turning point, pushed ahead by a growing demand and held back by endogenous and exogenous factors. 2024 statistics show a significant and sustained traffic growth, partially but not exclusively explained by the post-Covid catch-up. With more than 4,9 billion passengers, 2024 will likely be a record-breaking year, way beyond the latest forecast and above the 2019 pre-Covid level. According to the IATA and major players' experts, passenger traffic could reach 8 to 10 billion at the horizon 2040,[2] which urges airports to develop new tools to fluidify the growing passengers' flow. At the same time, the air transport sector faces headwinds in relation to environmental concerns and geopolitical issues.

- The aviation sector is on a slower decarbonizing trend than rail, maritime or road transport due to technical challenges. Even though environmental lobbies are quite active in Europe, their actual impact on the growth of the sector is not significant for the time being.
- International tensions and especially the Russia-Ukraine war or the Middle-East conflict result in significant consequences on air transport such as border closure, or airspaces bans.
- Epidemic or pandemic risk is still present and could have a sudden impact on air transport like it had in March 2020.
- Finally, security threats, especially terrorism, remain at a very high level worldwide.

These major industrial, economic and policy challenges are incentivizing stakeholders to adopt a cautious approach in the development of a new identity management system.

Navigating this fast-moving and complex environment is a key condition to achieve interoperability of DTC standards and broad adoption. The successful implementation of the DTC, in return, might be a "missing link" in air traveler management systems, with the potential to boost airport security and support the growth of air transport by facilitating cooperation across operators, airports, and public authorities, as suggested by the results of the first pilot implementation of these innovative systems.

2. HOW THE DTC SYSTEM CHANGES IDENTITY MANAGEMENT IN THE AIR SECTOR

a. High-level introduction to DTC

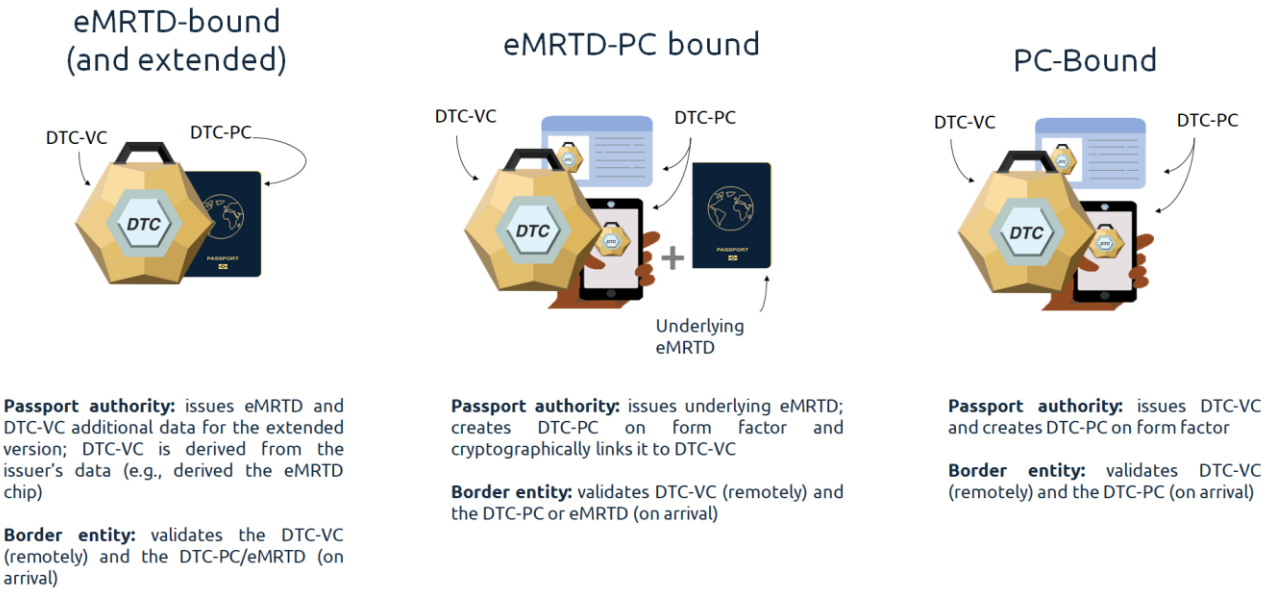
The DTC is a travel authentication certificate in a digital form initiated by the ICAO. It has been designed to act as a digital representation of the traveler's identity, temporarily or permanently replacing a conventional e-passport.

At its core, the DTC consists of a Virtual Component (VC), a piece of data containing typical passport information such as holder's biographical and biometrical information. The VC is cryptographically linked to an e-passport or a physical device beyond the traditional e-passport booklet, such as a smartphone or a smart card. While they are at the center of the current identity management system, these physical items, referred to as Physical Components (PCs), become optional in the DTC system. The concept is not revolutionary as it builds on the current structure of e-passports, which essentially already combine a VC, the cryptographically signed chip data, with a PC, the physical booklet embedding the chip and mechanisms to bind it to the VC.

DTCs will be issued by the relevant Issuing Authorities using the same processes as those for eMRTDs. They can exist independently or be derived from existing travel documents, replicating the identity and cryptographic data of the original eMRTD.

ICAO has proposed four distinct types of DTCs based on how the VC is created and linked to physical components:

1. **eMRTD-bound**: in this type, the DTC-VC is created using the data from an existing eMRTD acting as the DTC-PC. This DTC type is self-derived, i.e. anyone holding a biometric passport can technically generate the VC.
2. **eMRTD-bound extended**: similar to the eMRTD-bound type, this version also includes additional signed data beyond what is already available in the eMRTD.
3. **eMRTD-PC bound**: here, the VC is derived from an existing eMRTD but is linked to a different physical component such as a smartphone. The eMRTD remains functional and can act as a backup.
4. **PC-bound**: in this type, the VC is created independently by the Issuing Authority and linked to a physical component other than an eMRTD, such as a smartphone or a smartcard. No eMRTD is used as backup in this case.



Overview of ICAO DTC types, issuance and validation[3]

b. The trust framework supporting DTCs

The trust framework behind DTCs is established using the same Public Key Infrastructure (PKI) that underpins the security of current eMRTDs as specified by the ICAO. This global framework ensures interoperability between countries and enables travel credentials to be universally accepted.

A PKI is a system of procedures, cryptographic tools and protocols that manages public key certificates and pairs of public/private keys to provide data integrity and authenticity. The use of these key pairs allows issuing authorities to digitally sign the data embedded in travel credentials such as eMRTDs and DTCs in a secure, verifiable, and thus trustworthy manner. This ensures that the identity and biometric data contained in the travel credential cannot be altered or forged.

When a DTC is issued or derived by an issuing authority, it contains a data package signed with the issuing authority's private key. The digital signature acts as a seal of authenticity and integrity, assuring any verifier that the DTC originates from a trusted source and was not tampered with. For the verification, the verifier uses the authority's public key is used. This enables verifiers such as border controllers, airlines and others to confirm the validity of a DTC without having to interact with the issuing authority.

A critical enabler of this trust framework is the ICAO Public Key Directory (PKD). While private keys are unique to each issuing authority and are securely kept to ensure the authenticity of DTCs, the PKD is the centralized, secure platform that facilitates the sharing of public keys and public key certificates among countries for the verification of the digital signatures on eMRTDs and soon DTCs. It avoids cumbersome bilateral exchanges between countries and facilitates trustworthy border verifications.

By leveraging the same infrastructure as eMRTDs, DTCs inherit a proven and globally trusted security framework. However, unlike eMRTDs, where the physical passport booklet (i.e. the DTC-PC) is a trusted and controlled component issued by the authorities, the trustworthiness of the DTC-PC varies depending on the type of DTC. In some cases, such as a DTC hosted on a personal device like a smartphone, the DTC-PC is not directly controlled or issued by the authorities, raising concerns about how border controls will assess the authenticity and integrity of such devices and thus, the DTC itself. Moreover, for eMRTD-bound DTCs, their verification can be conducted entirely digitally, as only the digital signature of the passport data is verified, with potentially no need to check any PC. This marks a significant shift from the traditional reliance on authority-issued physical travel documents.

c. Main applications & added value

The DTC system has broad potential applications in the air transport sector and beyond. Considering only flight-related applications, in most of the situations today, a passenger on an international journey from A to B has to prove his/her identity at several stages: airport entrance security control, flight check-in, baggage-drop, departure immigration control, security screening, aircraft boarding, arrival immigration/visa control, customs inspection… Those multiple and repetitive verifications significantly contribute to extending the travel overall duration, explaining that it's highly recommended to arrive at airports 2 to 3 hours prior to the departure time of the flight. It also contributes to an increase of airport frequentation, resulting in several congestion points, heightened security risks, significantly higher airport facilitation costs, passengers' stress and fatigue.

As previously mentioned, with passenger's flow expected to double by 2040, the implementation of the DTC system could simplify and speed up air traveler management across stages. Instead of being verified at each travel step, the passengers' identity and other relevant data could be digitally shared with a first validator, then shared with the different entities distributed along the travelers' journey: airport authority, airline, screening staff, immigration / police at state of departure and state of arrival, customs…

This federated validation of the DTC, together with the deployment of facial recognition at each counter, could bring to an end the repeated identity document presentations and lead to significant time and cost savings, without compromising on security. The DTC system may support saving and selectively sharing additional data enabling new use cases improving a traveler's experience, for instance automatic baggage loss or delay claims, critical health information, backup travel documents in case of loss of the physical component (PC)…

Finally, non-flight related applications can also be part of the DTC scope such as airport transfers, duty-free access, accommodation booking and leisure activities.

3. CURRENT LEGISLATION & PILOT PROJECTS

The implementation of the DTC system requires amendments to the existing legal framework, at the international, EU and domestic level. It is also worth noting that as a border crossing system, DTCs do not only apply to air travel but could be extended to terrestrial or maritime transport, beyond the jurisdiction of ICAO. DTC pilot projects involving several countries have already been conducted and assessed, providing some important insights on the future that is to come for identity management in the air industry.

a. ICAO current legislation on travel documents

The ICAO is a specialized organization of the UN, gathering 193 contracting States and headquartered in Montreal, Canada. Following the provisions of 1944 Chicago Convention (sp. art. 37), the ICAO aims at unifying the civil aviation legislation of its Contracting States.[4] For this purpose, the ICAO adopts standards and recommended practices — SARPs — in the 19 different areas featured in the annexes of Chicago Convention. Standards are always mandatory, and Contracting States have to transpose them, if necessary, into their domestic legislation. Recommended practices are simpler, general guidelines that Contracting States are free to comply with or not. Frequently, a standard derives from an original recommended practice.

Travel documents are covered by Annex 9 of the Chicago Convention focusing on facilitation. Its article 3.11 reads that "*all passports issued by Contracting States shall be machine readable in accordance with the specification of doc. 9303, part 4"*. Machine readable passports are mandatory worldwide, where eMRTDs, containing biometric information stored on a chip, are not. Nevertheless, Annex 9 refers to eMRTDs in its article 3.9, providing that "*when a Contracting State issues an electronic Machine-Readable Travel Document (eMRTD), it shall do so in accordance with the specifications in Doc 9303"*.[5]

Following a similar strategy, the ICAO has been officially working on a common standardization of the DTC technology, in close collaboration with the International Organization for Standardization (ISO), since 2017. While DTCs may not become mandatory for Contracting States, the ones wishing to implement DTCs will have to follow the ICAO specifications to ensure interoperability of newly issued documents.

Up to now, ICAO's Traveler Identification Program working groups–the New Technologies Working Group (NTWG) and Implementation Capacity Building Working Group (ICBWG)–have developed guidelines and specifications for the DTC-VC and DTC-PC based on an underlying eMRTD (eMRTD-bound DTC). Their current focus is on the transmission protocol and other DTC types, but no documentation has been released yet.

b. IATA Initiatives

Unlike ICAO, IATA is a trade association representing 340 airlines around the globe. As a private but very influential player, IATA issues factsheets, recommendations and guidelines,

applying to its members and oftentimes followed by the rest of the industry. Since 2022, IATA has launched its "One ID" recommended practice (ref. 1701o and 1701p), featuring a DTC-like system based on the World Wide Web Consortium (W3C) Verifiable Credential model,[6] aiming to digitize the relation between the passenger and the airline from end-to-end, integrating with all the private and government stakeholders involved in air travel. Within the frame of One-ID, "*the passenger can digitally demonstrate to the airline that they have all the required documents to travel (passport, visa, other documentation) and that these documents are valid"*.

Notwithstanding their degree of observance throughout the air sector, IATA guidelines or recommended practices are never mandatory.

c. EU Legislation

On top of its existing regulations dealing with digital identity, such as eIDAS and eIDAS 2,[7] the European Union implements a specific regulatory framework for travel and digital ID documents. The key principles are contained in the Schengen border code (EU regulation n° 2016/399), different EU regulations, and the Frontex guidelines.

In a nutshell:

- The Schengen border code provides general conditions for third party nationals to enter within the borders of any Schengen member State (29 states incl. 25 from EU). The regulation refers to eMRTDs.

- EU regulation n° 2252/2004 defines standards for security features and biometrics in passports issued by EU Member States. Its provisions expressly refer to ICAO document 9303.

- The EU is preparing for the launch in 2025 of two new borders' crossing automated systems, using previously registered data and eMRTDs: the Entry/Exit System (EES) and the European Travel Information and Authorization System (ETIAS). Those two projects have been elaborated independently from the ICAO initiative on the DTC system.

- Frontex (the European border and coast guard agency) issued in 2015 its *Best practice technical guidelines for automated border control systems*, a document made of technical specifications and also referring to ICAO document 9303 as far as eMRTDs are concerned.

- More generally, with the eIDAS 2.0 regulation n° 2024/1183, the EU lays down the rules for a European digital identity wallet which could hypothetically store verifiable credentials and act as a DTC in the future.

d. DTC pilots

Pilot 1 – Conducted on request of the European Commission by the Netherlands with the KLM airline, on flights from Canada (5 airports) to Amsterdam from January to March 2024, this pilot project involved around 1500 passengers holding passports from Belgium, Canada and the Netherlands.[8]

Participants in the pilot have loaded the DTC-VC from their e-Passport onto their mobile device.

The experience, conducted at a reduced scale, was successful and outlined the following conclusions:

- The use of DTCs has the potential to enhance the end-to-end fluidity of air travel and translates into high satisfaction levels for the pilot participants.
- DTCs allow significant time savings, with processing time at the e-gates of Amsterdam airport being cut in half.
- There is a need for comprehensive legislation at the EU level to harmonize the implementation of DTCs across Member States.
- There is also a need for industry standardization to ensure successful creation, storage, and transfer of DTCs on *all* mobile phones.

Pilot 2 – Conducted by Finland with Finnair between September 2023 and March 2024 on flights between Helsinki and more than 20 international destinations mostly outside the EU, this pilot was run on a smaller scale than pilot 1 above.[9]

That pilot also turned out to be successful with a significant improvement of the time spent by passengers at border check: it took on average over 30 seconds for travelers with a physical passport to go through inspection, between 20 and 25 seconds for the ones going through automated border control with their eMRTD, and under 10 seconds for the travelers using DTC verification as part of the pilot.

4. ONGOING TECHNICAL, LEGAL AND POLICY CHALLENGES

a. Multiplicity of stakeholders

The implementation of the DTC system on the medium/long run involves a significant number of diverse stakeholders, both public and private, some international, others located in a specific jurisdiction, including but not limited to: the ICAO, the EU commission, national authorities in charge of civil aviation, of border control/immigration, of data protection, airlines, airports, international associations of airports and airlines (ACI, IATA…), IT companies…

Each of the stakeholders might have diverging interests and hold its own views on the DTC system. For instance, some stakeholders might place a very high value on personal data protection, while others would see in DTCs an opportunity to enforce strong security measures and surveillance mechanisms. From an economic point of view, stakeholders relying heavily on external airlines might not align perfectly with the ones belonging to a thriving national ecosystem and promoting their interests… This diversity of actors is both the reason why the adoption of common standards is necessary and challenging.

b. Fragmented and incomplete regulatory framework

As rapidly described points 3.a to 3.c, the regulatory landscape is incomplete and fragmented. To our best knowledge, there are no jurisdictions nor organizations offering complete legal grounds for the implementation of the DTC system today. This implies the necessity to change the current legal framework at ICAO, EU and domestic levels.

Considering only the security and data protection issues raised by the DTC system, the establishment of a harmonized legal framework will no doubt take considerable time and effort. Moreover, the DTC initiative at ICAO raises legal questions that go far beyond the aviation sector since the suggested changes would impact identity management across terrestrial and maritime borders. Dealing with the future of DTC systems is, consequently, dealing with sovereignty.

c. Recurrent security concerns

Security is probably the most important challenge relating to the launching of the DTC system. All stakeholders agree that the DTCs' level of security should be at least as high as the one of eMRTDs. Questions and challenges are numerous in this domain but mostly revolve around the authentication of the data contained in the VC, and the control of the public authorities on the DTC creation. Safeguard mechanisms where national authorities have, at any time, the possibility to reimpose physical controls at borders seem to be crucial to mitigate the effects of potential cyberthreats and system failures such as:

- *Identity theft and travel document abuse.* The loss or theft of a DTC-PC containing a DTC-VC can result in identity theft and fraudulent travel.

- *Enrollment of a genuine DTC by an imposter.* Attackers may attempt to enroll a legitimate DTC on their own device, impersonating a genuine traveler.

- *Sole reliance on biometric authentication.* Authenticating a traveler using only the DTC-VC and biometric matching, without verifying the DTC-PC, may lead to false acceptance.

- *Compromise of private keys in the DTC-PC.* Attackers could clone or forge valid travel credentials, enabling them to cross borders undetected.

- *Eavesdropping and unauthorized data sharing*. Accidental or intentional leak could expose private data, allowing attackers to misuse genuine DTC for fraudulent travel.

- *Compromise of cryptographic algorithms.* Current algorithms are not quantum-resistant, posing a future cybersecurity risk. ICAO and ISO are actively working on replacement solutions.

The development and deployment of the DTC system at an international scale also call into question the mutual trust between States: will State A trust DTCs created in B and *vice versa*?

Finally, the security and the reliability of the device acting as PC in the DTC system can be questioned. The lack of standardization of mobile phones worldwide, especially when it comes to the storage of encrypted data and encryption keys, together with their potential vulnerability to external threats, is a serious concern for policy makers in this domain. This also highlights the potential economic and technical inequalities when it comes to safely accessing the DTC system. Relying on devices designed, manufactured and sold by private companies for official identity management instead of publicly issued supports is the continuation of a broader trend of digitization but remains a paradigm shift when it comes to border control.

d. Protection of privacy

Unsurprisingly, the elaboration of the DTC system raises many important privacy and data protection questions. DTCs deal with information related to identifiable persons and thus fall under existing regulations protecting personal data in many jurisdictions.

For instance, in the EU, the 2016 General Data Protection Regulation (GDPR) regulates data collection and prohibits by default the use of sensitive data (pertaining to biometrics, religion, ethnicity, criminal prosecution…). Sensitive data treatment is allowed, among other exceptions, "for reasons of substantial public interest […] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".[10]

In addition to this general framework, the Passenger Name Record EU Directive regulates the transfer of passengers' data for the aviation sector, from the collecting airline to member States, and from the latter to third countries.[11] The EU Court of justice has a very strict interpretation of the text and regularly rules that it cannot be used in the absence of an actual or foreseeable terrorist threat.

The articulation between the future DTC system and the strict regulatory data protection framework needs to be considered especially if the state of departure and the state of arrival do not share common standards regarding the collection and transfer of personal data. The extraterritoriality of personal data protection in the aviation sector is the subject of an open and vivid debate. For example, in contrast to GDPR as explained above, in the United Arab Emirates (UAE), biometric data is widely used for automated border control and security

purposes, including for travelers coming from a jurisdiction with greater data protection, with local regulations granting authorities broader powers to collect and process such data.

Besides, as previously mentioned, part of the value-added of the DTC system lies in the potential combination of commercial and personal identification data and its transfer among different public and private stakeholders. The trend towards monetization of data by airlines and other stakeholders and the challenges to data protection it raises shall also be taken into consideration. To that regard, the participation of national and international public organizations in the standardization working groups (the German BSI and Luxembourg INCERT in ISO, national governments and the EU, the UN, the UNHCR in ICAO…) is essential to the elaboration of a system compatible with digital rights currently protected by national and international law.

e. DTC interoperability and associated costs

The implementation at a large scale of the DTC system requires very precise common technical standards and implies significant initial investments for States, airports, airlines and other players, for instance in biometric recognition equipment. ICAO works on this question (sp. document 9303) will for sure constitute a solid basis, but the risk of asymmetric standards and incompatible implementations is difficult to eliminate even in the long run. Obviously, asymmetry means potential friction in the traveler's experience, lesser efficiency, and potential security threats.

f. Social acceptability

Pilots conducted recently have shown that passengers, at least those involved in the pilots, were quite satisfied with this test phase. Social acceptability is nevertheless yet another potential constraint to the development of the DTC system at a larger scale since:

- A share of the potential users might be reluctant to digitization as a process eliminating human interaction.
- Some would not trust the efficiency and safety of the DTC system as a whole.
- Others may fear inappropriate transfer, leakage, or unlawful usage of their personal data.
- Finally, passengers could oppose the DTC system because of the perceived risk of non-reliability of their PC (mobile phone) and require an eMRTD back-up.

It is worth noting that a gap is likely to appear between frequent business travelers, generally more accustomed to innovations within airports and who might appreciate the time savings brought by the DTC system the most, and occasional travelers, who could be less convinced by the actual utility of this new technology and be less willing to go through the effort of creating their DTC while their eMRTD already answers most of their basic needs.

POLICY RECOMMENDATIONS

- **Multiply pilots and diversify the scopes**

DTC experiences should be **conducted on a larger scale, involve more diverse stakeholders, and better evaluate**, through qualitative and quantitative data collection, the positive impacts of DTCs, its costs, and social acceptance.

- **Unify the legal framework across jurisdictions**

A **unique DTC legal framework consistent with existing ones** (Schengen Border Codes, ETIAS/EES, eIDAS, GDPR) should be adopted in collaboration between public and private stakeholders, aligning at least EU legislation, ICAO future SARPs, and IATA RP.

- **Preserve privacy and user control in DTC usage beyond borders**

To deliver on its promise of efficient identity management and improved experience across the aviation industry, DTCs and their usage must be developed within a framework of trust. The use of DTC information outside border control shall be governed by the **highest standards of privacy and empower users to selectively consent** to the treatment of sensitive, personal, but also commercial data. Ensuring that only the necessary data is shared for a given purpose, preventing overexposure and reinforcing user protection is a *sine qua non* success condition.

- **Maintain physical passports**

Physical Components, in the form of an **e-Passport should be maintained as a safeguard security measure**, at the very least during the initial rollout of DTC. Public authorities should be the primary issuers and verifiers of DTCs.

- **Start with a limited scope**

DTC should be launched with a **limited scope of embedded data, then extended based on first feedback and stakeholders' needs**.

- **Think beyond aviation**

Terrestrial and maritime border crossing raises identical challenges and should be included in the roadmap for DTC development.

[1] In particular, following the ICAO specifications included in Doc 9303, which was initially titled "A Passport with Machine Readable Capability" in 1980, and which has been updated several times until the current 8th edition "Machine Readable Travel Documents" of 2021.
[2] *Global Air Passenger Demand Reaches Record High in 2024,* IATA, 30 January 2025. Press release.
[3] Adapted from Figure 5 in High-Level Guidance: Explaining the ICAO Digital Travel Credentials V1.0 (ICAO, June 2024), with minor modifications.
[4] "Convention on International Civil Aviation (Chicago Convention)." signed on 7 December 1944, last updated in 2006 with its 9th edition (Doc 7300/9)
[5] "Annex 9 to the Convention on International Civil Aviation: Facilitation." 16th ed., International Civil Aviation Organization, July 2022 (applicable from November 18, 2022).
[6] "Verifiable Credentials Data Model v2.0." W3C Candidate Recommendation Draft, W3C, 25 February 2025.
[7] Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, recently amended by Regulation (EU) 2024/1183, establishing the European Digital Identity Framework.
[8] "DTC1 pilot in the Netherlands", final evaluation report for the Dutch Ministry of Justice and Security, May 30, 2024.
[9] More information about this project on the dedicated page on the Finnish Border Guard website.
[10] Article 9 of Regulation (EU) 2016/679 (General Data Protection Regulation).
[11] Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime