Eurosmart's feedback on digital travel documents

Introduction to Eurosmart's feedback

Eurosmart would like to thank the European Commission for the opportunity to provide feedback on this crucial topic. Digital travel documents have the potential to make travelling much easier and smoother for EU citizens. For this reason, Eurosmart would favour a legislative act that lays down obligatory digitalisation of travel documents and facilitation of travel (options 5 and 6). A legislative act based on option 5 would allow all EU citizens to benefit from the usage of Digital Travel Credentials (DTC) when travelling in/via the EU Member States, as well as in all other countries supporting DTCs in conformance with the upcoming ICAO specifications. Eurosmart also recommends exploring option 6.

Options 1 to 4 should not be chosen for the digitalisation of travel documents and travel facilitation in the EU for the following reasons:

- Options 1 and 2 deviate from the ICAO DTC specifications, which will lead to interoperability issues, i.e., digital travel documents issued by the EU Member States cannot be used outside the EU and, vice versa, digital travel documents issued outside the EU (e.g., based on ICAO DTC) cannot be used in the EU Member States.
- Option 3 chooses just one of the 3 DTC Types defined by ICAO. These DTC Types support different use cases and have different requirements for the citizen's mobile device. Choosing just one DTC Type limits the supported DTC use cases and restricts the usage to citizens possessing certain devices.
- Option 4 (digitalisation of travel documents on a voluntary basis) deprives many citizens of the benefits of DTCs. The citizens of a Member State not issuing DTC Types 2 and 3 cannot use these DTCs Types at all, and citizens in possession of any DTC Type cannot use these DTCs while travelling in/via Member States not supporting DTCs.

I. Scope and objectives of the future legislation

Mandatory for Member States, voluntary for users

Eurosmart recommends that the European Commission draft ambitious legislation that will greatly facilitate travel across the EU and beyond. In this respect, it is of the utmost importance that the legislation includes:

- Mandatory issuance of digital travel documents: so that all EU citizens can use them.
- Mandatory facilitation rules when crossing borders with digital travel documents: to foster usage and ease travelling at large.

- Compatibility with existing standards, including ICAO DTC: to ensure interoperability within the EU and with the world. This paper further develops this point in sections III and IV.

Thus, options 5 and 6 are the best-suited options to achieve the objective of facilitating travel across borders.

Nevertheless, EU citizens should have the choice of whether to have or use a digital travel document. Therefore:

- The choice to have a digital travel document shall be left to the holder.
- The choice to use a digital travel document shall be left to the holder.

Therefore, the former facilitation infrastructure and process shall be maintained.

Types of documents in the scope

Member States shall issue digital travel documents for all physical travel documents, including:

- National identity cards;
- Passports;
- Laissez-passer;
- EU residence permit so that their holders could enjoy the same level of facilitation when moving within the EU/Schengen area and crossing external borders;
- Schengen Visa so that their holders could enjoy the same level of facilitation when moving within the EU/Schengen area and crossing external borders. In that case, the digital travel document may be bound to the holder's passport (provided it is chip-based).

Regarding national identity cards, Eurosmart notes that the European Commission's Inception Impact Assessment refers not only to a **digital passport** but also to a **digital identity card** based on the ICAO DTC specifications. The scope of the ICAO DTC specifications is restricted to traveller identification only, i.e., the digitalisation of the travel document application of electronic passports and other travel documents, such as identity cards. Any other feature of an identity card, as well as all use cases besides traveller identification, are out of the scope of the ICAO DTC specifications. Therefore, the scope should be restricted to the **travel document application of an identity card** instead of the identity card as a whole.

Keeping physical travel documents

Digital travel documents cannot replace physical travel documents. The latter shall remain. Issuing authorities shall keep issuing physical travel documents and keep the existing infrastructure for their control. Digital travel documents shall supplement physical travel documents but not replace them. The rationale is the following:

- ICAO DTC does not provide for storage of fingerprints in an interoperable manner, unlike chip-based physical travel documents (e.g., passport, national identity card…). This may be an issue where reinforced checks are needed (another biometry than the portrait is needed).
- A high level of resilience of border crossing shall be ensured. In particular, it shall still be possible for individuals to cross the border if the device (e.g., mobile phone) where the digital travel document is stored has been hacked, damaged or is out of battery without altering in

any manner the trust in the identity verification. In these situations, physical travel documents are a necessary fallback solution.

II. Key principles to reach a high level of trust

The first key principle is that digital travel documents shall be exclusively issued by a public authority and not by a private entity. This way, digital travel documents would truly reflect the same level of trust as passports.

The second key principle is that there should be no compromise on security. Eurosmart has concerns regarding what could be a long regulatory process, with many actors having different perspectives in terms of security, potentially leading to low security because of compromise. Digital travel documents must protect user data at a similar level as chip-based travel documents (e.g., electronic passports). The legislative text should harmonise the security level across the EU to avoid identity theft and impersonation. New possibilities for identity fraud must be analysed, and their possible impact, for example, the digital manipulation of face photos (morphing). The text should accordingly set the main security principles and empower the European Commission to adopt implementing acts referencing specific security standards.

The text should also mandate security certification of the physical component of the digital travel document implemented in the mobile device (e.g., SIM, eSIM or secure elements present in smartphones). Such a security certification is particularly important because the digital travel document is cryptographically bound to this physical component in the mobile device. The certification should be performed at a level "high", as defined in the Cybersecurity Act. In other words, the device must resist attacks from attackers with high attack potential. Third parties must perform security certification with oversight from national cybersecurity certification authorities.

The third and last key principle is maintaining and leveraging existing infrastructures to rationalise costs and benefits.

III. Reliance on ICAO's work, including ICAO DTC Types 1 & 2

The legislation should rely on ICAO's *Guiding Core Principles*[1]. When it comes to the DTC specifications as such, the legislation should rely on ICAO DTC Type 1 and Type 2 and discard DTC Type 3:

- The eMRTD bound DTC (Type 1) is the fallback for citizens who do not possess a suitable mobile device. DTC Type 1 allows sharing data online in a standardised format before travel. DTC Type 1 consists in duplicating (except for additional biometrics such as fingerprints) and sharing the content of the chip-based travel document. As such, its deployment is very simple and could be achieved easily and quickly. DTC Type 1 will be very useful for implementing online transactions in an interoperable manner whereby the travel document data can be shared with a third party ahead of the journey.

- The eMRTD-PC bound DTC (Type 2), i.e., a DTC Physical Component, which also hosts the DTC Virtual Component, is the preferred solution. DTC Type 2 is a step further. It still supports online transactions (as described above in the case of DTC Type 1) but also allows offline transactions in an interoperable manner. DTC Type 2 is used in addition to the physical document, which can be used in all situations where DTCs are not supported or where a higher level of security is required, and the physical security features of the document need to be checked. DTC Type 2 can be installed on citizens' mobile devices that meet the functional

[1] ICAO, Guiding Core Principles for the Development of Digital Travel Credential (DTC), Version 4.4, October 2020.

requirements of the ICAO specifications (and the EU's security requirements, as explained in the following Section IV).

- The PC-bound DTC (Type 3), i.e., a replacement of the physical travel document, appears not to be a viable option for at least two reasons. Firstly, a physical travel document continues to be required for worldwide travel. Secondly, the lack of binding of the digital travel document to a chip-based travel document raises several issues that may hamper the trust in the claimed identity. In addition, it creates a dependency (and potentially a subordinate relationship) of the issuing authorities to device manufacturers. This situation may be very questionable as the latter may be ruled by laws from foreign countries, meaning the issuing country is not sovereign in the issuance and usage of digital travel documents. Moreover, some device manufacturers enjoy monopolistic positions on the market, which may spur them to impose their views and choices. Thus, DTC Type 3 should not be retained.

IV. Pushing the limits of ICAO DTC: the EU's role in ongoing standardisation activities

The ICAO DTC specifications are still under preparation, and the requirements are regularly revisited in this process. The EU should promote its views in the context of this process to make sure that the ICAO requirements take the EU's expectations onboard. For instance, the scope of the ICAO DTC specification should be extended in order to support the worldwide interoperability of DTC solutions. The EU must advocate before ICAO the need to extend the DTC standard. For this purpose, the European Commission can rely on its representative and EU national representatives taking part in the ICAO NTWG.

The EU should ensure that ICAO specifications include the following elements:

(1) Transport protocols (offline use), such as BLE (BlueTooth Low Energy), UWB (Ultra-wideband) or Wi-Fi Aware, solving the shortcomings of NFC;

(2) Fully standardised online transactions, based on ISO/IEC 23220. The scope of the ICAO DTC specifications is so far restricted to the DTC data structure (DTC-Virtual Component) and the interface between the border control station and the DTC Physical Component. For interoperability reasons, the interface for transmitting the DTC data over the internet (e.g., online transactions) needs to be standardised as well. This interface can be used to upload DTC data in advance of travel to allow for any pre-checks, to upload DTC data in a travel authorisation process, for airline check-in etc.

More precisely, regarding the transport protocols:

- Current draft specifications for the device (e.g., mobile phone) to which the digital travel document is cryptographically bound only consider NFC as a physical transport protocol to exchange the data in the course of an offline transaction. This technical choice will create substantial shortcomings. NFC used by a mobile device to present a digital travel document provides a much lower level of user experience and reliability than a chip-based travel document while still requiring substantial investments to upgrade the infrastructure to support this new use case. Therefore, alternative physical transport protocols should absolutely be considered (1) solving these blocking points, (2) offering the same level of reliability as NFC used with chip-based travel documents and (3) ensuring a shorter or equal transaction time. In that regard, BLE, UWB or Wi-Fi Aware are very interesting candidates that should be integrated into the ICAO technical specifications. The standard ISO/IEC 18013-5 "Mobile driving licence

(mDL) application" prepared for the mobile driving licence should be considered a starting point for offline use. Firstly, it covers the same features as the ones targeted for digital travel document Types 2 and 3, namely support of offline transactions and cryptographic binding between the digital data and the physical device. Secondly, it has demonstrated its uptake and fitness, which allowed numerous deployments of mobile driving licenses worldwide that are interoperable and support BLE and Wi-Fi Aware. Besides, this interoperability has been demonstrated through various interoperability events.

The priority is to address all the above-mentioned issues at the ICAO level. As a fallback solution, the EU should tackle these points by drafting EU technical specifications supplementing the ICAO ones.

Besides, ICAO specifications do not cover security requirements. Thus, the EU legislation will need to rely on technical specifications covering the security requirements that should be met by the mobile device (e.g., mobile phone) to which the digital travel document is cryptographically bound.

The **schedule** for the legislative act needs to consider that the ICAO specifications are still under preparation. Before adopting these specifications, it is best practice to perform international interoperability tests between different DTC and DTC reader implementations – as previously done for physical travel documents such as passports. This testing serves as proof of the technical concept, including the usability by citizens and border guards, as well as quality assurance for the specifications. The EU should actively support these interoperability tests. In addition, ICAO test specifications need to be prepared for conformance testing to enhance DTC implementations' interoperability.

Some pilots were already announced in Europe, for example, between Finland and Croatia, and between the Netherlands and the USA. Pilots are also run outside Europe (Canada-USA, New Zealand-Australia, UAE, South Korea etc.). The EU should take the outcome of these pilots into consideration for any future initiative. In particular, the EU should consider the learnings on the user experience, user acceptance and travel facilitation.

V. Compatibility with European Digital Identity Wallets

The EU rules on digital travel documents and travel facilitation must consider the ongoing initiative to set up a European Digital Identity Wallet (revision of the eIDAS Regulation).

Firstly, the digital travel document shall leverage the EU Wallet. The Wallet aims to ensure a high-security level and protection of the data it holds. Therefore, it is paramount to mandate the storage of the digital travel document in the Wallet.

Secondly, the digital travel document shall take the shape of a Qualified Electronic Attestation of Attribute (QEAA) as introduced by eIDAS 2. Moreover, because of the very nature of digital travel documents, it is of the utmost importance to protect access to its authentic source, which is very sensitive, but also access to the private key used to generate the attestation representing the sovereignty of the state in the digital world. For these reasons, the issuance of digital travel documents shall be subject to supplemental requirements compared to what will be required for issuing QEAA. In particular, it shall include at least the followings:

- Digital travel documents shall be exclusively issued by a public authority and not by a private entity.
- Digital travel document issuance shall be subject to supplemental security requirements.
- Very strong security requirements on digital travel documents shall be enacted to avoid identity theft/impersonation. In particular, a mandatory security certification pursuant to the

EU Cybersecurity Act at level "High" shall be required for the device (e.g., mobile phone) to which the digital travel document is cryptographically bound.

VI. Exploring option 6

The facilitation measures proposed in option 6 have the potential to substantially increase fluidity, streamline and expedite border crossing while increasing the traveller experience and the throughput of airports. Therefore, option 6 should be promoted and implemented, provided strong data protections are guaranteed to EU citizens. This implies that the following conditions are met:

(1) Option 6 shall supplement the current facilitation measures, which shall remain.

(2) Option 6 shall be made available in a dedicated area that is well delineated and signalled. For example, a biometric corridor or an entry or exit lane dedicated to travellers that have subscribed to this service.

(3) Travellers shall have previously consented to use the system (through registration).

(4) Travellers shall have the possibility to revoke this consent at any time.

The implementation of this option may require substantial investments from national authorities or airport operators. Therefore, these facilitation measures shall only be mandated where the flow of travellers is sufficient. The idea would be to avoid heavy investments at border crossing points with a low number of travellers.

In addition, it is worth noting that there are different degrees of "seamlessness" that will lead to different implementations in the field. A risk-based approach needs to be set up. The degree of seamlessness should be commensurate with the risk profile of the traveller.

Annexe: Assessing the different options in the light of five criteria

This Annexe defines five criteria for comparing the different options.

Criteria definition

Criteria	Definition
Harmonised security level high VAN.5	Security level high is harmonised across the EU and involves third party security certification and oversight by national cybersecurity certification authorities
Clear timeline	A clear timeline is set and enforced
Harmonised standards	Legal documents clearly identify standards to avoid fragmentation and non-equivalent security solutions; this includes protection profiles.
Clear EU mandate	EU rules that mandate the digitalisation of travel documents and travel facilitation measures, including the possibility to adopt implementing acts to ensure a harmonised implementation in the field
Compatibility with ICAO DTC	The Regulation clearly refers to ICAO DTC and covers all use cases
Compatibility with eIDAS	The legislative text clearly refers to the eIDAS Regulation

Comparison

This table presents a comparison of the different scenarios based on the five criteria.

Criteria	#1	#2	#3	#4	#5	#6
Harmonised security level high VAN.5	x	x	p	x	p	p
Clear timeline	x	x	x	x	p	p
Harmonised standards	x	x	p	x	p	p
Clear EU mandate	x	x	x	x	OK	OK
Compatibility with ICAO DTC	x	x	OK	x	OK	OK
Compatibility with EUDIW	x	?	?	?	?	?

Legend:

- x not met
- OK met
- p partially met
- ? not clear

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, TrustSEC, WISekey**, **Winbond, Xilinx**), laboratories (**SGS Brightsight, CCLab, CEA-Leti, Jtsec**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ETSI, ECSO, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com