Classification: Public

EWC D2.1

Digital Travel Credential (DTC) for EUDI Wallets

WP2

Author: SICPA SPAIN

Contributors: Gen, Amadeus, Circletree.eu

Day of submission: 06/12/2024

Contents

Revisions

Version	Date	Author	Changes/ process
v1.0	07-11-2024	SICPA	Close to final version sent to the wider EWC consortium for feedback.
v1.1	11-11-2024	SICPA	Final version sent to EWC coordinators, ready for sharing with HADEA, DGCNECT and DG HOME
V1.2	06-12-2024	Coordination Team	Approved by Management Board and Coordination Team. Final quality check.

List of abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
EAA	Non-Qualified Electronic Attestation of Attribute
API	Advance Passenger Information
ARF	Architecture and Reference Framework
CBOR	Concise Binary Object Representation
DTC	Digital Travel Credential
EDIR	European Digital Identity Regulation
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
ETIAS	European Travel Information and Authorisation System
EUDI	European Digital Identity
F2F	Face-to-Face
FAQ	Frequently Asked Questions
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
MRTD	Machine Readable Travel Documents
NFC	Near Field Communication
PAD	Presentation Attack Detection
PID	Person Identification Data
QC	Qualified Certificate
QES	Qualified Electronic Signatures
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
TCN	Third Country Nationals
TSP	Trust Service Provider

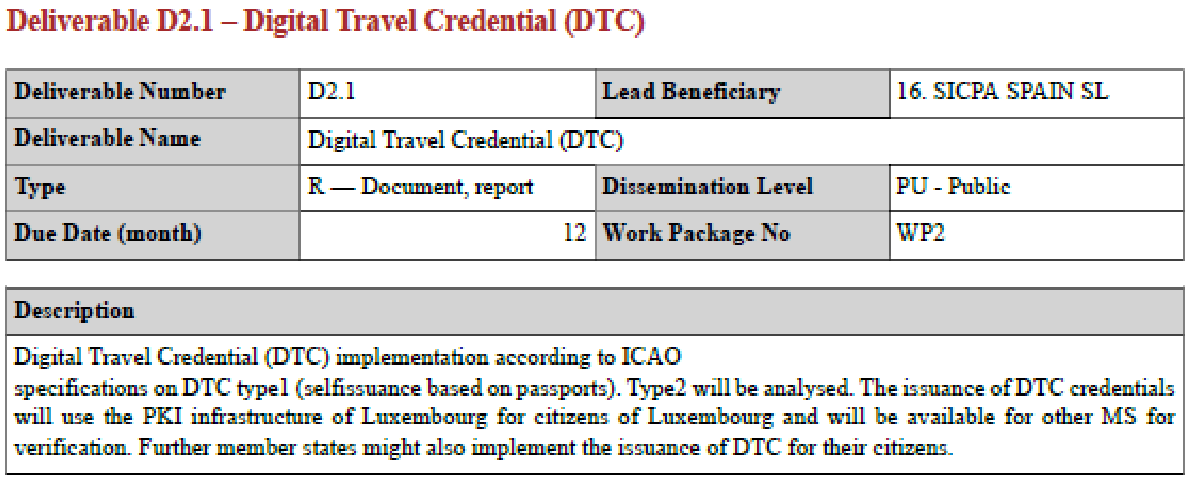
1. Executive Summary

As the European member-states are going to issue EUDI wallets and new digital identity credentials (e.g. PID), the industry is requesting those member-states to also issue credentials in which the Passport attributes (e.g. name, surname, date of birth, ID picture,…) can be used securely by relying parties as part of their regulatory obligations (e.g. for airlines having to collect Advance Passenger Information) and automated searches of personal data (e.g. for border control authorities). The objective is that those credentials can be consumed both by border authorities and the industry at large, which means compliance to ICAO and EU ARF standards and specifications.

While the legitimacy of such requirements by the industry, border authorities and by end-users is well recognized, the way to implement the issuance and verification of such credentials is challenged by technical limitations and current legal frameworks both on European and national levels. The aim of that deliverable (D2.1) is to assess potential implementation approaches, piloting opportunities and define actions plan and recommendations to enable such credentials to facilitate travels within the EU and potentially abroad.

2. Introduction

Description from Grant Agreement



Deliverable D2.1 – Digital Travel Credential (DTC)

Deliverable Number	D2.1	Lead Beneficiary	16. SICPA SPAIN SL
Deliverable Name	Digital Travel Credential (DTC)		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	12	Work Package No	WP2

Description
Digital Travel Credential (DTC) implementation according to ICAO specifications on DTC type1 (selfissuance based on passports). Type2 will be analysed. The issuance of DTC credentials will use the PKI infrastructure of Luxembourg for citizens of Luxembourg and will be available for other MS for verification. Further member states might also implement the issuance of DTC for their citizens.

What is the business rationale behind this scenario, why was it prioritized?

Nowadays, passports are broadly used by the industry (e.g. banks, airlines, hotels, telcos, etc.) to comply to national and European regulations requiring identity proofing. When interacting online, relying parties must base their assessment on the physical document which is very cumbersome for users as it requires the scan of physical documents that is both expensive, time consuming and error prone. While ICAO could potentially propose technical solutions and specifications for such credentials, the mandate of ICAO is to satisfy border operations and not requirements from the industry at large. Therefore, with eIDAS 2.0, the EU Commission has a great opportunity to solve that issue and give tools to the industry to consume passport data while complying with the GDPR regulation. Finally, a credential containing all passport attributes will be used very often (similarly as one often presents its physical passport) by citizens which will contribute to adoption of EUDI wallet.

As the number of related transactions is very important, EWC decided to prioritize this scenario and demonstrate its feasibility in various contexts and market verticals.

3. Current State of the Art (SotA) and challenges

In October 2020, ICAO has issued specifications regarding the standards and implementation of the Digital Travel Credential (DTC)[1]. The aim of this innovative concept is to decrease the time for processing data from the e-passport chip at security gates.

The DTC consists of a Virtual Component (DTC-VC) containing the digital representation of the holder's passport data and a Physical Component (DTC-PC) that is cryptographically linked to the Virtual Component.

DTCs were defined in three types, including:

1. Type 1 DTC (Derived from a Physical Passport)

Description

- Type 1 DTC is a digital version of a traveller's physical passport data derived from an existing, valid passport. The traveller still needs to carry the physical passport during travel, as the DTC serves as an additional, digital proof of identity.
- In accordance with the guiding principles, an eMRTD bound DTC is considered to be issued by a Travel Document Issuing Authority, because it is derived from the Authority's data
- The traveller MUST have their physical eMRTD in their possession while traveling.

Use Case

- This type of DTC is useful for easing identity verification, especially in automated or remote check-in processes, but requires the physical passport to be on hand for final checks at border control.

2. Type 2 DTC (Digital Equivalent of a Physical Passport)

Description

- Type 2 DTC is also derived from a physical passport, but the physical device (mobile phone) serves as the DTC-PC, with the eMRTD as the alternate or as a fallback.
- The virtual component will be an exact copy of the electronic document data.
- The traveller SHOULD have their physical eMRTD in their possession while traveling.

Use Case

- Type 2 DTC could be used in jurisdictions or scenarios where a full digital passport equivalent is accepted, enabling fully digital cross-border travel. However, the traveller still needs an issued physical passport to derive the DTC from, but it is not required to be present during travel.

3. Type 3 DTC (Fully Digital Travel Credential)

Description

- Type 3 DTC is a purely digital travel credential that does not rely on or is derived from a physical passport. It is intended to function as a fully digital passport, managed and issued by the relevant national authority.
- There SHALL be a distinguishable identifier to recognise the document as a virtual credential without an eMRTD as an alternate or as a fallback
- May have its own document characteristics (ID [passport] number, validity period, digital signature, etc).

[1] Guiding Core Principles DTC

Use Case

- This type represents the future of fully digital identity for international travel, where travellers can cross borders with just their digital credentials. This type of DTC requires countries and international authorities to recognize and accept purely digital passports, which is still in development. DTC Type3 is intended to serve as a complete replacement for the physical passport during travel. It contains all necessary passport data digitally, allowing the traveller to leave their physical passport at home.
- Type 3 could also be a good solution as "Temporary digital Passport" in case someone loses its passport just the moment before travelling.

Current challenges

As protecting borders is directly related to country's national security, the ICAO Digital Travel Credential (DTC) Guiding Core Principles devote rightfully much attention and great care to the ICAO DTC's data authenticity, integrity and the authentication thereof.

An ICAO DTC MUST be at least as secure as an eMRTD. To achieve this, the DTC data is signed by the issuing authority's public key infrastructure (PKI) and MUST be used in combination with the physical document (for type1). This design makes the DTC secure (perfect for border crossing), but compromises data privacy and flexibility, blocking many other high value use cases in the digital travel journey, such as:

- online booking & check-in
- seamless baggage drop
- security area access
- lounge access
- boarding planes or ferries
- post arrival car rental
- hotel room registration and key collection
- …

In the context of digital transformation of society, the ICAO DTC Guiding Core Principles does not satisfy current and emerging market needs from the industry to comply to national and European regulations enforced by many different jurisdictions and sectors, especially those related to data privacy and flexibility. Moreover, in certain national regulations like the German Passport Act[2], the industry is not allowed to access to the data stored on physical documents chip. Also, the current format of the DTC does not allow for selective disclosure on an attribute granularity level like required by GDPR (art5 c) regulation[3].

Regarding user-experience, the current eMRTDs are used in a very cumbersome manner providing poor data quality for relying parties like airlines or hotels that need to check those documents as part of their regulatory requirements. Indeed, travelers have to enter their passport details manually or by scanning the Machine-Readable Zone (MRZ) and then scanning the passport chip if allowed in the related jurisdiction. This is leading to a lot of errors and extremely bad user-experience for travelers and users.

Last but not least, ICAO DTC technical specifications are not compatible with EU ARF wallet specifications[4] and therefore not consumable by relying parties that are part of the EU digital identity eco-system. By introducing the EUDI wallet, the focus around data is shifting from

[2] Passport Act (PassG)

[3] Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR)

[4] Architecture and reference framework - EUDI Wallet

the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities. As such, the revised eIDAS regulation (2.0) is addressing the privacy and flexibility market needs. Importantly, the eIDAS regulation also establishes a legal framework for the use of Person identification Data (PID) and (qualified) electronic attestations of attributes ((Q)EAA). This legal basis is essential for the adoption and appropriate issuance, use and verification of digital identity data and related attributes across Europe.

The eIDAS EWC project has the ambition to bring both worlds together to create exciting digital travel journeys for travelers and to unlock business opportunities in the travel domain and broader in the industry. The most important data elements that need to be covered are personal data (e.g., name DoB, etc.), passport data (e.g. document nr. and expiry dates) and biometric data (passport picture or other facial image).

4. Proposed solution

Various options have been evaluated to meet all stakeholders and use-cases requirements:

Option A

A dedicated PhotoID credential (following ISO/IEC 23220-2/4 specifications to be published) would be issued by the member states travel document issuing authorities. It would contain all passport data attributes signed individually one by one with the same certificates used for eMRTDs and as optional the unwrapped version of the passport chip Data Groups (namely DG1, DG2 and DG16).

Pros: It would fit both border authorities and industry requirements while using both the trust framework of ICAO (PKD) and the EU Architecture Reference Framework. Indeed, for border control operations, a DTC compliant with the ICAO specifications could be reconstructed by downloading the various unchanged Data Groups from the PhotoID credential. The DTC could then be stored by the border authorities in a gallery to be used in combination with the physical document to facilitate verifications at the gate. Also, the PhotoID credential could provide relying parties from the industry (e.g. banks, airlines, hotels, telcos, …) means to access passport data to comply to national and European regulations in their domain while complying to GDPR at the same time.

Cons: As this ISO/IEC specifications are currently in draft mode, it remains difficult for stakeholders to base their strategy on that credential. Also, there is currently no regulation issued either by DGHome or by member states that would require governments and travel document issuing authorities to issue such credentials. Finally, the EU ARF does not yet provide guidance clarifying whether QTSPs would be allowed to issue such credentials and if yes, under which conditions and for what use-cases (border control authorities would not accept such a credential if issued by a QTSP). Last but not least, ICAO New Technology Working Group (NTWG) would have to support this approach before it could be used in the border control context, even if it compliant with DTC Type1 requirements.

Option B

A PID credential (PID+) would contain as optional attributes all or part of data elements of the passport chip (additional attributes only and not a dedicated credential as such).

Pros: existing legal framework for PID using compatible technical specifications compatible in EU. It will fully cover the industry requirements.

Cons: It is not a travel document and cannot support the border control use-case (at least outside Schengen area).

Option C

A credential that would contain the unwrapped version of DTC according to ICAO specifications and would be signed by the states travel document issuing authorities with the same certificates (CSCA) used for eMRTDs. (specific QEAA – requires a QTSP for the issuance).

Pros: It will use the trust framework of ICAO (PKD).

Cons: However, despite the fact that the DTC contained in the credential is technically compliant with ICAO specifications, the fact that it is re-signed (even if it is the states travel document issuing authority) seems to be problematic from the point of view of ICAO. Indeed, it would be seen as a new type of identity document and a dedicated specification (eg DTC type2) would have to be published in order to be used in a border control context. We can imagine that EU member states could issue this credential to be used by the industry in the hope that ICAO would follow that proposition for the specifications of a DTC type2 at a later stage.

Other big issue with that approach is that, for the industry, it is not fit for purpose because all attributes are shared in a proof request and selective disclosure is not supported at an attribute level of granularity as requested by GDPR.

Option D

A DTC compliant with the ICAO specifications would be downloaded and stored in the EUDI wallet without any further modifications.

Pros: The DTC could be used in a border control ecosystem in combination with the physical eMRTD

Cons: specific formats/protocols would have to be implemented within the EUDI wallet to download, store and share it with border authorities. Those protocols would not be compliant with ARF specifications and therefore could not be used in other context like check-in, …. The industry and end-users will have to use current eMRTD reading technologies to comply to their regulatory requirements as today.

What makes the envisioned EUDI wallet supported journey better than the current journey (SOTA)?

As demonstrated in the EU barometer on that topic[5], a majority of Europeans are in favor of the use of digital documents when travelling to or outside the Schengen Area.

The adoption of such travel credentials is coming with strong expectations for a good user experience and high security. Therefore, the technical implementation needs to comply to those requirements on top of complying to ICAO and EU ARF specifications. From all those scenarios, option A concept seems to be the most promising as it can support both requirements from border authorities and the industry at large while meeting specifications from

[5] Digitalisation of travel documents and facilitation of travel - September 2023 - - Eurobarometer survey

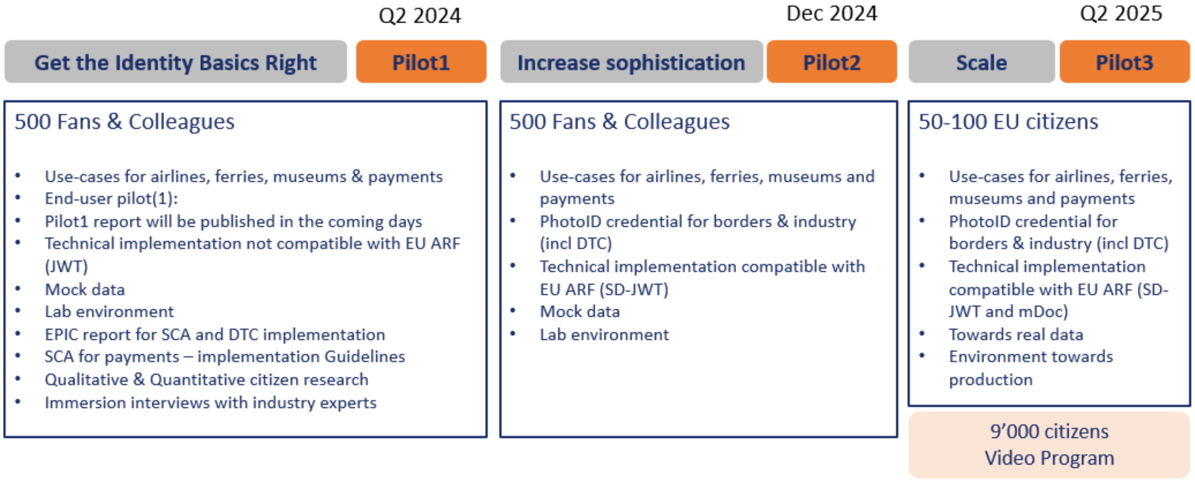
ICAO and from the EU. This eco-system of digital travel credentials could be applied to both EU citizens and 3rd country nationals (TCN). This could notably support DGHome strategy and vision regarding EU digital travel app[6][7] and issuance of a new regulation[8]. The user experience is greatly simplified, and it might positively impact the adoption of EUDI wallet by citizens. Indeed, this credential would provide a clear incentive to citizens to on-board in this new digital identity eco-system to simplify their digital transactions. We have discussed and validated the proposed approach in different workshops where organizations like DGHome, EULisa, member-states representatives, wallet providers, airlines representatives were involved. Now, the concept of PhotoID needs to be tested in various context and use-cases to collect insights and feedback from end-users and main stakeholders. This is what we aim to demonstrate in the pilots to come.

5. Pilot setup

The overall objectives of the pilot are to demonstrate the following points:

- Attributes from the Passport/PhotoID can be shared to any relying party including: member states, border authorities within and outside of the Schengen area, airlines, airport security, hotels, banks,
- Attributes from the PhotoID can be shared to any relying parties in a secure and data privacy preserving manner thanks to a selective disclosure mechanism.
- The user experience is smooth, efficient and quick
- Usability and pertinence of SD-JWT format for online transactions
- Demonstrate that attributes from the PhotoID credential can be shared in a proximity (phase3 only) and remote verification context

The WP2 from EWC responsible for travel & payments has organized three phases for piloting all associated use-cases:



Q2 2024

Get the Identity Basics Right — Pilot1

500 Fans & Colleagues

- Use-cases for airlines, ferries, museums & payments
- End-user pilot(1):
- Pilot1 report will be published in the coming days
- Technical implementation not compatible with EU ARF (JWT)
- Mock data
- Lab environment
- EPIC report for SCA and DTC implementation
- SCA for payments – implementation Guidelines
- Qualitative & Quantitative citizen research
- Immersion interviews with industry experts

Dec 2024

Increase sophistication — Pilot2

500 Fans & Colleagues

- Use-cases for airlines, ferries, museums and payments
- PhotoID credential for borders & industry (incl DTC)
- Technical implementation compatible with EU ARF (SD-JWT)
- Mock data
- Lab environment

Q2 2025

Scale — Pilot3

50-100 EU citizens

- Use-cases for airlines, ferries, museums and payments
- PhotoID credential for borders & industry (incl DTC)
- Technical implementation compatible with EU ARF (SD-JWT and mDoc)
- Towards real data
- Environment towards production

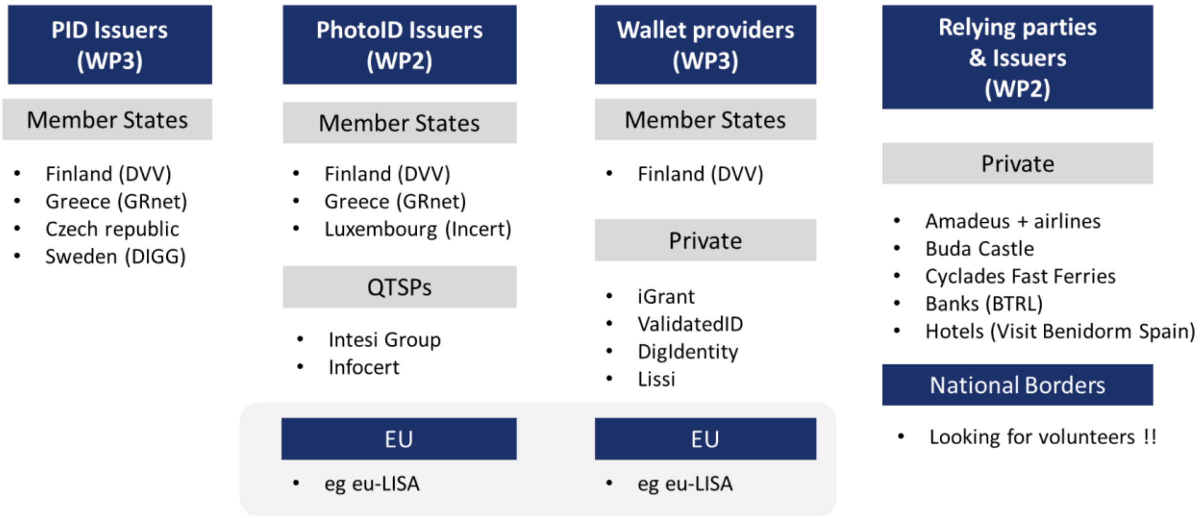
9’000 citizens
Video Program

[6] Commission proposes to digitalise passports and ID cards for easier and safer travel in the Schengen area - European Commission

[7] Commission proposes an EU Digital Travel application

[8] eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=cellar:e6f41083-8643-11ef-a67d-01aa75ed71a1

In order to pilot those use-cases, a whole eco-system of stakeholders has been put in place. An overview is given in the below schematic:



PID Issuers (WP3)

Member States

- Finland (DVV)
- Greece (GRnet)
- Czech republic
- Sweden (DIGG)

PhotoID Issuers (WP2)

Member States

- Finland (DVV)
- Greece (GRnet)
- Luxembourg (Incert)

QTSPs

- Intesi Group
- Infocert

EU

- eg eu-LISA

Wallet providers (WP3)

Member States

- Finland (DVV)

Private

- iGrant
- ValidatedID
- DigIdentity
- Lissi

EU

- eg eu-LISA

Relying parties & Issuers (WP2)

Private

- Amadeus + airlines
- Buda Castle
- Cyclades Fast Ferries
- Banks (BTRL)
- Hotels (Visit Benidorm Spain)

National Borders

- Looking for volunteers !!

While Phase1 was implemented in a lab environment and on JWT format because of time constraints from EU ARF specifications delivery, Phase2 will comply partially to EU ARF specifications by implementing all credentials on SD-JWT format. This will allow all stakeholders to adapt their technical stacks and run interoperability tests to ensure consistent implementation of remote verifications across the consortium. The objective for Phase3 will be to include as well mDoc format for remote and proximity verifications.

EWC will pilot for the first time the use of PhotoID, perfectly aligned with both ICAO specifications and the Europeans ARF requirements, in use-cases involving relying parties from the industry. A similar setup has been used in a proof-of-concept (PoC) lead by IATA and involving two passengers using different digital wallets and travel credentials on a round-trip between Hong Kong and Tokyo[9].

In EWC context, a sample of EU citizens will be offered the possibility to use a EUDI wallet from a private or member state provider to store and share travel credentials and experiment a streamlined travel experience, thus demonstrating the potential of PhotoID in the context of travel within the EU.

[9] IATA - Fully Digital Travel Experience Closer to Reality

6. Learnings, recommendations and risks

In the context of addressing implementation rule books on the topic of Digital Travel Credential, the following learnings and recommendations should be taken into account:

Technical specifications

- T1: General requirements
    - Selective disclosure is needed from the industry to comply with data minimization requirements from EU GDPR regulation on data privacy.
    - DTC does support selective disclosure only on a Data Group level which means that it would not be compliant with GDPR regulation on data minimization.
    - ARF supports two file formats (SD-JWT and mdoc) that are not compatible with DER used for DTC.

- T2: DTC type1, if implemented with the PhotoID approach, would satisfy both the requirements from border authorities and from the industry. Considering the operational challenges for the implementation of DTC type1, border authorities and the industry at large should focus on this latest type. DTC Type1 implementation in operation would be a very important step towards full digitalisation even if the physical and digital versions of the passport will co-exist for a long time.

- T3: Interoperability is achieved on thanks to the technical standards and also through the alignment on data structures and definitions. In order to compare names, surnames or date of birth, the data formats need to be aligned across member states. Typically, the character sets and transliterations from different national versions require a global alignment to be machine readable like the data used in passports chips. This will ensure that relying parties do not need to implement all different flavors of name spellings. The international standard that has demonstrated to be successful since more than twenty years is ICAO Doc 9303, and more specifically part3. It is of upmost importance that personal data are stored in the PhotoID with this international standard and the implementation rulebook on that topic should take this into account. More details are highlighted in Annex A.

- T4: Usage of DTC in the border crossings context is benefiting from the security that is associated with the physical component embedded in the physical document (passport chip). No equivalent on mobile devices has proven yet to provide the same level of assurance and it is probably not foreseeable in the coming five years. Therefore, the approach remains to link the DTC to the physical document and travelers will still have to carry their physical documents when crossing borders for the next ten years at least.

- T5: Currently, the specification describing the DTC transmission protocol is missing. To our knowledge, this specification is currently being discussed by ICAO New Technology Working Group (NTWG) and is expected to be published in 2025. EWC will implement it if available during the lifespan of this project.

- T6: While PhotoID approach is, on our opinion, compliant with ICAO specifications on DTC type1, the implementation of PhotoID by EU member states should still be coordinated with ICAO New Technology Working Group (NTWG). The objective would be to receive the endorsement of such an approach from NTWG to avoid any misalignment with ICAO. Therefore, we recommend to initiate workshops with NTWG representatives from EU member states and then to the larger NTWG representatives community.

- T7: SD-JWT format for credentials is well suited to perform online and remote transactions guaranteeing data privacy when sharing data attributes with relying parties

Legal

- L1: The issuance of the PhotoID must be done by each member states Travel Document Issuing Authority being the authentic source, having direct access to the passport civil registry and providing a high trust to relying parties.

- L2: QTSPs and wallet providers should be able to issue PhotoID credentials to persons that do not have PIDs but have passports (e.g. children, non-EU citizens, …) with level of assurance high. This credential would only cover use-cases from the industry and not be usable in the border crossing context. Wallet providers could have a commercial interest to provide this service to their users for adoption purposes. The business incentive for QTSPs though remains less obvious.

- L3: The European Commission should evaluate the benefits of providing a European wallet for 3rd Country Nationals, immigrants to benefit from the same EUDI eco-system of verification within their travel and not just for their border crossing transactions. This would be part of the EU digital travel application as a wallet[10] and would allow 3rd Country Nationals to experiment a seamless registration at a hotel for example.

- L4: For the member states that have National Passport act (e.g. Germany[11]) preventing the industry at large to access passport attributes from the chip, a modification of the law is necessary. The modification would adopt the principle of consent management and data minimization from GDPR to regulate the access to personal data without forbidding it[12] [13]. Alternatively, a European policy on that topic could harmonize various national implementations.

User experience

- U1: Relying parties like airlines, ferries, hotels or banks are very interested in that approach and would trust it to streamline their operations. EWC is going to pilot relevant use-cases in different market verticals related to travel and demonstrate the benefits in the context of digital transformation of this industry.

- U2: Currently, users have to scan their physical passport for each digital transaction requesting their identity attributes, either with their mobile phone at home or with passport readers in a face-to-face verification. Most of the time, the exchange of data is even done manually, which is the source of many errors. With the PhotoID approach, users will have to scan their physical passport only once during the on-boarding phase.

- U3: Instead of entering manually passport attributes (e.g. document number, name, date of birth, …), users will be able to simply scan a QR code and give their consent to share their data with the relying party. This will avoid manual errors and will allow

[10] Commission proposes an EU Digital Travel application

[11] Passport Act (PassG)

[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Légifrance

[13] Disposición 16673 del BOE núm. 294 de 2018

relying parties to verify the authenticity, integrity and validity of the data. This is a major paradigm shift in digital transformation of the travel industry.

Risks

- R1: One perceived risk is that this new tool could benefit fraudsters, criminals and human trafficking. The biggest threat identified is actually during the on-boarding process and issuance of the PhotoID (eg morphed photos). PhotoID credential must be issued only to the legitimate holder of the physical travel document (eMRTD). Therefore, during the issuance process, the user must be authenticated with the PID of the EUDI Wallet user and through a “live selfie” where the user is compared to the Data Group 2 portrait stored on the ePassport chip. This should avoid impersonation fraud during on-boarding and issuance of the PhotoID and therefore limit the possibility of frauds.

7. Status of deliverable 2.1

Deliverable 2.1 was planned initially to be delivered for month12. We have sent a proposition of EPIC regarding this subject to DG CNECT in October 2023 and did not receive any feedback. As a result, we decided to change the approach. Indeed, we conducted interviews with different member-states to understand the constraints and with industry representatives (eg IATA) to collect requirements from the industry. Finally, we decided to organize a series of workshops with interested member-states representatives, DGHOME and EULISA. The first workshop was organized on 22nd April 2024 (by Teams) and the 2nd workshop has been organized on the 10th of June 2024 in Amsterdam (Hybrid). Those workshops received a very big interest and more than 60 people attended them either physically or virtually.
The objective is to converge towards a solution to be implemented and tested during that large scale pilot that would satisfy the requirements from the industry (compliance to regulations) and be as close as possible from existing standards issued by ICAO.
For phase1 of the user tests (June 2024), it was too early to have a concrete implementation of the proposed solution and we used synthetic data.
For phase2 (end of 2024) and phase 3 (2025), we intend to have a technical implementation of the above-mentioned approach with test-users that will provide insights on the usability and trust they could get from that experience.

This report corresponds to the deliverable 2.1 called Digital Travel Credential. A final report on that topic will be available at the end of the project mid-2025 and will comprise all insights collected during the pilots.

GITHUB link for open-source schema definition (SD-JWT format):
GitHub - sicpa-dlab/photo-id-vc: Verifiable Credential for a Photo ID.

EWC testbed – DTC proof of concept backend:
https://ewc-controllers.pre.vc-dts.sicpa.com/swagger-ui/index.html#/

8. Conclusions

In the current report, we have discussed about the various requirements from border authorities and the industry to access passport attributes. We have seen also the technical difficulties for the implementation and the challenging selection of standards to leverage trust eco-systems from ICAO and the EU. Finally, we have seen the legal blocking factors that limit the usage of EUDI wallet in the travel industry.

Various stakeholders from the EU commission (DGCNECT, DGHOME, EULISA), from member states (Finland, Sweden, Netherlands, Hungary, Spain, Luxembourg), from the industry (SICPA, Amadeus, Finnair, VISA, Cyclades Fast Ferries, Buda Castle, IntesiGroup, InfoCert, iGrant, DigIdentity, ValidatedID) and academic (UAegean) have given their inputs. The PhotoID (ISO) would be a good compromise and therefore has been selected for piloting within EWC. This concept covers requirements both from the industry and from border authorities. To make meaningful progress with regards to the user-experience that is key for adoption, we believe it's critical to take a use case by use case approach and test this concept in every market vertical. Our suggestion is to assess the following use cases in priority order:

1. Automation of filling API (Airlines)
2. Hotel registration process (Hotels)
3. Booking ferries tickets (Ferries)
4. Age verification (Museums)

The objective is to assess the feasibility of the technical implementation and collect insights for the improved user experience. This report and the final report can support the issuance of an implementation rule book on that topic to align specifications and legal frameworks across the jurisdictions and ecosystems of digital identity.

9. References

EU references

1. eIDAS 2.0 revision 2024
2. EUDI wallet Architecture and reference Framework (ARF) eudi-doc-architecture-and-reference-framework/docs/arf.md at main · eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework · GitHub
3. Collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls Carriages preview | Legislative Train Schedule (europa.eu)
4. Collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime Carriages preview | Legislative Train Schedule (europa.eu)
5. GDPR Regulation - 2016/679 - EN - gdpr - EUR-Lex (europa.eu)

ICAO references

6. Guiding Core Principles for the Development of Digital Travel Credential (DTC) Guiding Core Principles DTC (icao.int)
7. Digital Travel Credentials (DTC) ICAO-TR Digital Travel Credentials
8. ICAO 9303 Doc Series (icao.int)

IETF references

9. SD-JWT specifications draft-ietf-oauth-sd-jwt-vc-03 - SD-JWT-based Verifiable Credentials (SD-JWT VC)

ISO

10. PhotoID ISO/IEC 23220-2/4

National regulations

11. German Passport Act (PassG) – Section 18. Pt4 Passport Act (PassG)

IATA references

12. Supplementary Information for IATA W3C VC schema for Passport (Recommended Practice 1701p)

10. Examples of law texts

GDPR art 5

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

*(c) adequate, relevant **and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)**;*

ICAO 9303 part1, Ch2 Scope:

*Doc 9303 consists of various separate documents in which general (applicable to all MRTDs) as well as MRTD form factor specific specifications are grouped. See Section 5.1 “Doc 9303 Composition” for an overview. These specifications are not intended to be a standard for national identity documents. However, **a State whose identity documents are recognized by other States as valid travel documents shall design its identity documents such that they conform to the specifications of Doc 9303-3 and Doc 9303-4, Doc 9303-5 or Doc 9303-6**.*

Collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls article 4.3:

***Air carriers shall collect the API data referred to Article 4(2), points (a) to (d), of Regulation (EU) [API border management] using automated means** to collect the machine-readable data of the travel document of the traveller concerned. They shall do so in accordance with the detailed technical requirements and operational rules referred paragraph 5, where such rules have been adopted and are applicable.*

German Passport Act (PassG) – Section 18. Pt4

Passport Act (PassG)

Use in the private sector

1) Passports and passport substitutes may also be used as proof of identity in the private sector.
2) Serial numbers may not be used in such a way that it is possible to access personal data from data files or to link data files.
3) Passports may not be used for automated searches of personal data or for automated storage of personal data.
4) Transport operators may electronically read and process personal data from the passport’s machine-readable zone only if they are required by international agreements or entry regulations to assist with controls in international travel and to transmit personal data. Biometric data may not be read. The data shall be deleted as soon as they are no longer needed to fulfil these obligations.

11. Annex A – Convention for data structure and formatting

To achieve global interoperability, the primary and secondary identifiers in the MRZ shall be printed using upper-case OCR-B characters from [ISO 1073-2], illustrated below, without diacritical marks, and conform to the number of character positions available.

0123456789

ABCDEFGHI

JKLMNOPQR

STUVWXYZ <

Diacritical marks are not permitted in the MRZ. Even though they may be useful to distinguish names, the use of diacritical marks in the MRZ would confuse machine-reading equipment, resulting in less accurate database searches and slower clearance of travellers. If the national characters are not Latin-based, a transliteration into Latin characters shall be provided. The reference can be found in the following document:

ICAO Doc 9303 – part3 / 6. TRANSLITERATIONS RECOMMENDED FOR USE BY STATES

Transliteration tables for the most commonly used Latin, Cyrillic and Arabic families of languages are provided in this Section 6.

The issuing State shall transliterate national characters using only the allowed OCR-B characters and/or truncate, as specified in the form factor specific Parts 4 to 7 of Doc 9303.