IATA

Preview Paper: End to End Digital Identity Proof of Concept

Contents

Glossary

Digital Identity: Digital Identity is a term used broadly and can have different interpretations depending on the context or use. In general terms, Digital Identity is a set of electronically captured and stored attributes and credentials that can uniquely identify a person.

Verifiable Credential (VC): Verifiable Credential is a credential in a digital form. Examples of credentials and data contained in credentials may include:

- Biographic and biometric data from the passport or other identity document
- Visas, travel authorizations and residence permits
- Health-related status, contact tracing information (such as a Passenger Locator Form – PLF), digital arrival declarations
- Other captured verified biometrics (such as a face image or 'selfie')

Digital Wallet: Digital Wallet is an application that securely stores Verifiable Credentials, in such a format that the holder of the Digital Wallet can present or selectively disclose required data to any verifying party, such as to demonstrate admissibility to travel to an airline. Verifiable Credentials can be issued to the passenger's Digital Wallet by an airline, government authority or other 3rd Party authorized to issue.

Digital Travel Authorizations (DTA): DTA is an electronically enabled travel authorization that is designed to establish an interoperable framework and standardize the issuance of online visas, allowing travelers to enter foreign countries. DTA enhances the automation of the travel authorization process via creating an alternative to traditional paper visas.

Passport VC: Passport VC is the digital version of the physical document held in the form of a Verifiable Credential. It allows passengers to selectively disclose attributes to certain authorities.

DTA VC: DTA VC refers to the digital document issued to a traveler's Digital Wallet as an eTA approval (DTA) representing the individual's proof of authorization to travel in the form of Verifiable Credential.

Loyalty VC: Loyalty VC is a Verifiable Credential that holds the traveler's loyalty status from certain airlines. Loyalty VCs are pre-standard.

Order VC: Order VC is the digital document in the form of Verifiable Credential that holds traveler's order details. An Order VC as a credential stored in a digital wallet is pre-standard.

Introduction

IATA has been driving the Modern Airline Relating Program[1] and OneID initiative to transform passengers' retail and travel experience. As part of these efforts, the use of Digital Identity technology has been looked at across the passenger journey, from shopping to travel, to offer a more personalized, seamless, and secure travel experience.

Trusted Digital Identity Credentials - The Future of Secure and Seamless Travel

To support the industry with this transformation, IATA has been developing standards for a digital identity ecosystem that is interoperable between various aviation stakeholders, airlines, travel agents, airports, and governments.

IATA's standards are based on the use of W3C Verifiable Credentials (VC) and decentralized digital identity. Recently, IATA has released alpha specifications for the W3C VC schema for passport, visa, and the ICAO Digital Travel Authorization (DTA) for industry testing.

The End-to-End Digital Identity Proof of Concept (PoC) outlined in this paper will test these standards, and demonstrate that IATA's vision of a seamless journey using Verifiable Credentials is no longer a concept but a reality.

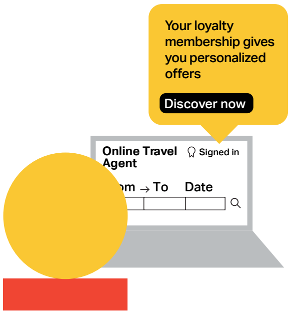
Summary of Modules

1. **Creation of Digital Identity Credentials.** The PoC assumes that the customer has already created their digital identity based on ePassport and holds other credentials, such as airline's loyalty status information.
2. **Retailing.** The PoC starts when the customer shops on an Online Travel Agent (OTA)'s mobile app. The customer uses their Loyalty Verifiable Credentials to obtain a personalized offer from different airlines. The PoC illustrates how a customer can receive recognition of their loyalty while using an OTA reservation system. Upon a successful order, an Order ID will be issued as a Verifiable Credential to the passenger's wallet.
3. **Service Delivery #1: Post-Booking.** The OTA offers the customer the opportunity to check their travel document requirements as a complimentary service. The customer agrees and shares only their nationality. Trip.com checks using Timatic and confirms that the customer only needs a valid passport to travel.
4. **Service Delivery #2: Check-In.** The customer consents to share their Order ID directly with the airline from their Digital Wallet and is guided through the check in process. The airline confirms the customer's admissibility to travel and offers a contactless journey at the departing airport. On the day of departure, the customer is then able to board the aircraft using their biometric without physically needing to present their passport or boarding pass to the gate agent.

Future Travel's Journey

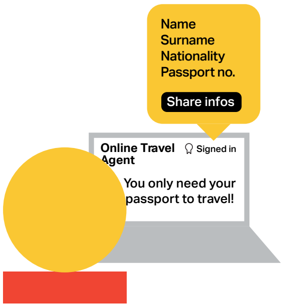
Retailing

Customer shops on an Online Travel Agent (OTA)'s mobile app, using their Loyalty Verificable Credentials to obtain personalized offers from different airlines. An Order is the issued as a Verificable Credential to the passenger's wallet post reservation.



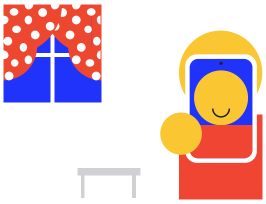
Post Booking

The OTA checks travel documents as a compli mentary service. The customer agrees and shares only necessary document portions. OTA checks and confirms that the customer only needs a valid passport to travel.



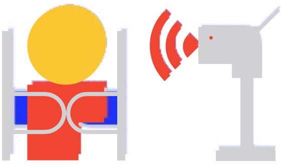
Check-In

Customer shares their Order with the airline from digital wallet and is guided through the check-in process, providing biometric information to opt in to contactless airport journey.



Contactless Travel Journey

On the day of departure, the customer is then able to board the aircraft without physically presenting their passport or boarding pass.



[1] iata.org/retailing

© 2023 International Air Transport Association. All Right Reserved.

Key Highlights of the PoC

The PoC illustrates interoperability throughout the entire travel value chain by incorporating various credentials, i.e. digital version of passport, live face image, loyalty programs, and order information. These credentials, issued and utilized by different parties for various purposes, exemplify the essential interoperability required within the industry's global network and travel value chain.

Simultaneously, the PoC emphasizes customer centricity, placing the passenger in control of their information. Passengers have the autonomy to decide which details they want to share with other parties. During the process, the passenger can opt to disclose only essential information, e.g. passport name, nationality and loyalty tier level, without revealing their complete passport or loyalty membership information.

Additionally, the PoC streamlines processes and enhances the passenger experience by enabling seamless sharing of relevant credentials from their digital wallet. This eliminates the need to manage multiple records, ensuring a hassle-free interaction with various services. Moreover, passengers can complete document checks remotely by sharing their credentials in advance. This allows the passenger to arrive at the airport 'ready to fly' and use biometrics for an efficient, contactless experience.

Partners in Design

Various stakeholders in the travel value chain contributed to the project, with the following roles and tasks:

Building blocks	**Contributors**
Airline partner	British Airways
Travel agent partner	Trip.com
Identity Verification/Digital Identity Wallet	IDnow
Passport VC	SICPA
Live Biometric Image VC	IDnow
Loyalty VCs	Verchaska
Trip.com mobile app mock-up	Trip.com
British Airways mobile app mock-up	AWS & Branchspace
Order VC	Verchaska
BA biometric process at boarding	Amadeus
Verification of VCs	Accenture

Creation of Foundational Digital Identity Credentials

A trusted digital identity credential can be created through a digital identity onboarding service provided by an issuer. The issuer software application undertakes the necessary checks, verifications and authentications that are needed to issue a trusted digital identity credential[2]. These steps are as follows:

1. **Preparation:** Traveler is in possession of their ePassport, digital wallet, digital identity services, and mobile device

2. **Machine Readable Zone (MRZ) Scanning:** Traveler opens their passport to scan their MRZ

3. **Reading the Chip in ePassport:** Through the Near-Field Communication (NFC) reading, the biometric and biographic data in the chip is obtained.

4. **Presentation Attack Detection (Liveness Detection):** The traveler's face is scanned for liveness verification, ensuring that the actual person is present and preventing any attempts to defraud the system.

5. **Document Authentication**: The authenticity of the document is checked to ensure the following:
   a. Identity is genuine (exists, valid, alive); presenter links to identity (unique, authority registered, sole claimant, not an imposter)
   b. Presenter (e.g. passenger) uses the identity in the community/system
   c. Document is valid and verified as genuine, unaltered and from a valid issuing authority
   d. Biometric Authentication: The biometrics in the passport chip is matched with the person in possession of the phone (1:1 match)

6. **Passport VC is issued** to the customer's digital wallet.

The other credentials, such as Loyalty Membership VC and Order VC, can be issued directly by the airlines and travel agents respectively and stored in the Digital Wallet.

Benefits Compared to the Current Process

There are notable benefits to the adoption of the creation of Digital Identity credentials, shown below:

- Opening the Possibility of End-to-End Digital Processes: During the air travel journey, passengers are required to share or show their passports multiple times to various stakeholders. The availability of a digital version of the passport opens the possibility of digitizing and automating this process.
- Enhanced Convenience: By managing their credentials in a digital wallet, passengers can easily access them whenever necessary, eliminating the hassle of dealing with different types of physical credentials.
- Increased Trust and Improved Data Quality: Due to the rigorous validation and authentication processes involved in creating a digital passport, airlines and governments can place higher trust in digital identity credentials compared to manual document checks. Accepting digital identity credentials also ensures improved data quality.

Technical Development

It is assumed that the creation of Digital Identity credentials is done beforehand; however, the Proof of Concept (PoC) did include the development of a Passport and Loyalty Verifiable Credential (VC).

For the Passport VC, all the steps mentioned above were undertaken, except for the ePassport chip reading, which was not conducted due to the lack of time. Regarding Loyalty VCs, three airlines' Loyalty VCs were created.

Future Maturing for Robust Standards

The ePassport chip reading should be available, where applicable, for the creation of the Digital Identity credential to ensure the authenticity of travel documents.

Additionally, airlines' ability to issue loyalty memberships as a VC to passengers' Digital Wallets requires further attention. While many airlines already offer a digital version of frequent flyer cards that can be stored in a mobile wallet, they may further benefit from expanding this to a W3C VC for wider use cases. To achieve this, the VC schema for frequent flyer memberships will be needed.

[2] Interoperability in the One ID Ecosystem Technology Guidance V1.0

Digital Identity in Retailing

The retailing module placed focus on testing the functionality of an order within the framework of Offers and Orders.

The passenger first shares only the tier level info of three airlines with the OTA, receives offers, chooses one, and subsequently shares the full loyalty membership as well as passport name with the OTA for order creation. Once the airline creates an order and passes it to the OTA, the OTA issues an Order VC to the passenger's digital wallet based on that order info.

The significance of decentralized digital identity shown in this module serves multiple purposes. Firstly, it acts as a safeguard to substantially minimize fraud risks for airlines by ensuring the authenticity of all participants in the travel value chain. This verification process is done to ensure that the stakeholders involved in an offer are genuinely who they claim to be. Additionally, the retail aspect empowers airlines to create personalized offers tailored to the individual consumers' preferences, indicated by the data provided through their digital wallet.

The module facilitates the transition away from legacy technologies, enabling a full reliance on Offers and Orders. It is worth noting that although this module was worked on pre-standard, closely with the IATA standards team, it played a large role in influencing the development of order schemas, pioneering standard creation in the Order management space.

Benefits Compared to the Current Process

There are many benefits to the retailing experience that comes with decentralized Digital Identity as opposed to today's current practices.

- **Better Understanding of Customers:** Airlines have a great advantage by having the ability to better know their customers, who they are and what they want, in the first place. This is a form of information and its sharing that has historically been inhibited by legacy systems. Better understanding their customers, regardless of the sales channels, allows airlines to better personalize their offers according to the needs and preferences of the customer.
- **Zero Knowledge Proof:** The use of VCs enables the consumer (in this case the OTA) to verify the proofs are true (for example that the passenger is a platinum tier member) without the need to know the data elements themselves.
- **Reduction in Fraud:** The digital verification of customer information allows for a reduction in fraud. A VC can corroborate the information the airline has on the traveler helping to reduce fraudulent transactions while providing better protective measures, both physical and financial for all the stakeholders in a customer's journey.
- **Simple, Seamless Process:** The complete booking process, for the passenger, is controlled within the single OTA provided application. There is no need to swap between multiple applications or other data sources. All required information is from and contained within the passengers existing wallet.

Technical Development

An Order VC was created for the retailing module. This credential included the Order ID issued by the airline. To simplify the issuance process, the Issuer as a Service API was employed, enabling the API consumer to issue a Verifiable Credential to the Wallet with just a single call. This approach eliminated the need for an in-depth understanding of the intricate workflows and standards associated with VC Issuance. The API will also be published on the IATA API Hub.

Future Maturing for Robust Standards

In the future, focus will be placed on these aspects of the PoC for standardization of Digital Identity in retailing:

- **Loyalty VC's Selective Disclosure:** Among the Loyalty VC attributes, the tier level info was supposed to be selectively disclosed to be shared with airlines for making offers. But this couldn't be delivered for this PoC, so a separate tier VC was used as a workaround.
- **Passport VC's Selective Disclosure:** The First/Last Name was supposed be selectively disclosed to be shared with airlines for making an order, but this also couldn't be delivered for this PoC. Instead, a separate First/Last Name VC was used.
- **Travel Agent's Ability to Receive and Process VCs:** In this case, the VCs were verified by one of the partners in the PoC before being passed to the OTA.
- **Travel Agent's Ability to Issue an Order VC:** In the PoC, an actual Order VC was issued by the OTA using another partner's issuer service.

© 2023 International Air Transport Association. All Right Reserved.

Service Delivery #1

After the order is created, the OTA offers the passenger to check travel documents. If the passenger agrees they then share their nationality as it is the only info the OTA needs in checking travel requirements. Travel requirements are checked, and the OTA informs the passenger that only a valid passport is needed for travel.

Benefits Compared to the Current Process

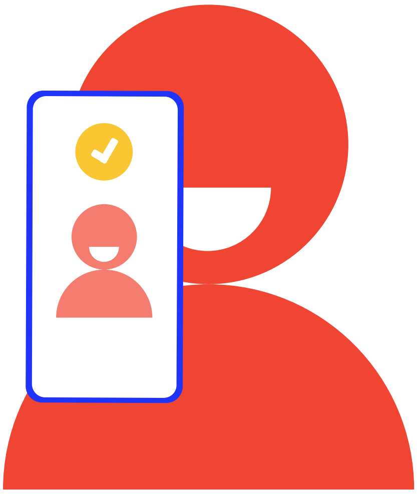
Leveraging Verifiable Credentials to share trusted travel information in advance brings many benefits. Sharing Digital Identity credentials can be extended to additional services, such as travel requirement checks for passengers, ensuring a consistently simple and seamless experience.

Technical Development

In the developed system, communication with the passenger in the flow was established: the OTA checks travel documents and informs the passenger about the results promptly.

Future Maturing for Robust Standards

Selective disclosure for Passport VC, specifically intended for nationality, was planned but couldn't be implemented in the PoC. As an alternative, a distinct nationality VC was employed. In the PoC, the travel agent's capacity to receive and process VCs was not executed, but it remains a potential consideration for future developments.



Service Delivery #2

One day prior to departure, equivalent to today's check-in timeframe, the airline checks passenger's travel documents remotely and offers a contactless process at the airport. Airlines are required to collect passports and other travel documents information from passengers. However, in this specific scenario, only a passport is necessary. Additionally, because the booking was made through a travel agency, the airline also needs the passenger's Order information to access the booking details. Therefore, passengers are requested to provide both the Order and passport information during the check-in process.

After confirming that the traveller is ready to fly, the airline presents an option for a contactless process at the departing airport. To encourage participation, the airline may highlight the benefits, including reduced queueing time and a seamless experience. The passenger is informed about the need to share a biometric image and boarding pass information. In this specific scenario, since the airline manages biometric handling at airport touchpoints, only the biometric image is necessary. The passenger agrees and provides consent, proceeding to share the required biometric image with the airline.

On the day of departure, the passenger is identified using biometrics, allowing them to pass through the boarding gate without the need to show documents to an agent, and subsequently board the plane seamlessly. These processes align with the One ID end-state, advocating for digitalized document checking and a contactless experience at the airport.

Benefits Compared to the Current Process

By leveraging Digital Identity credentials and biometrics, passengers enjoy the following benefits:

- **Simple, Easy Travel Journey:** Passengers do not need to deal with various records and proof in different formats; they can simply share those records and proof from their Digital Wallet. This removes the need to re-enrol every time they travel. They can simply share their already created digital credentials whenever needed.
- **Off-Airport Process:** Passengers can complete the check-in process prior to departure and arrive at the airport 'ready to fly'. They do not need to queue at the airport to see a check-in agent and can go straight to drop off their bags.
- **Ambiguity Avoidance:** By being offered a contactless process in advance, passengers have better visibility of what to expect at the airport in terms of the process.
- **Seamless, Contactless Process:** Passengers do not need to show their physical documents at each touchpoint at the airport and can use biometrics to procced.
- **Less Privacy Concern:** Passengers understand what information needs to be shared with whom and opt-out is available.

© 2023 International Air Transport Association. All Right Reserved.

Technical Development

A temporary Live Biometric Image Verifiable Credential (VC) was generated, capturing a live face during the Digital Identity creation process specifically within presentation attack detection. This Live Biometric Image VC can be stored in the passenger's Digital Wallet and shared with the airline for the contactless process.

When the passenger arrives at the airport touchpoints, their face image is compared against the previously received live biometric image.

The airline we partnered with conducted trials of biometrics boarding at T5 Heathrow. During the trial, passengers enrolled their Live Biometric Image during check-in to participate. The airline then built a gallery of images for the corresponding flight. At the airport, the passenger's face was captured and matched with the gallery; a successful match allowed access through the gate. In contrast, for the PoC, to demonstrate interoperability, the airline used the biometric image received from a passenger without requiring a separate enrolment.

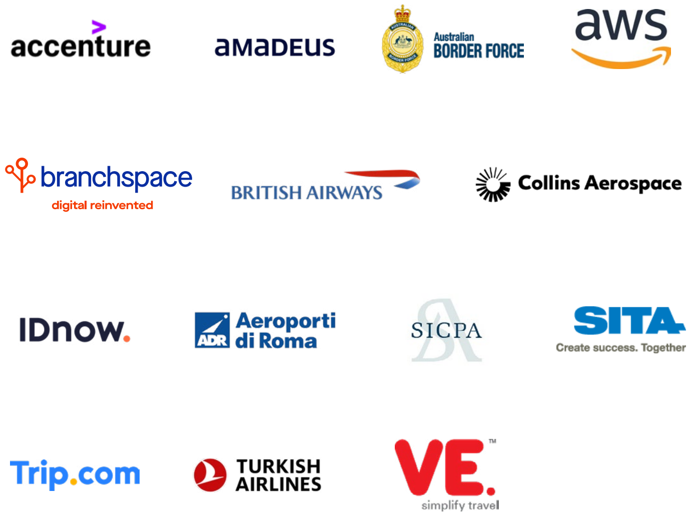
Future Maturing for Robust Standards

Throughout the PoC, there was no information exchange regarding the airline's ability to receive Order and Passport credentials from the passenger's Digital Wallet for processing. To enable this functionality, airlines should develop the capability to receive these credentials from the passenger's Digital Wallet and utilize them for processing. Additionally, the airline needs to determine whether a contactless process is available at specific airports and can help establish a connection between the passenger and the relying party responsible for organizing the contactless process. Airlines, due to their direct communication with passengers closer to departure, are ideally positioned to offer such services. For global adoption of a contactless process, it is essential that airlines are aware of airports providing this service and connect their customers with the relevant relying parties. Industry standards and recommendations in this area will be examined in 2024.

Furthermore, there is a need for the development of standard schemas for Live Biometric Image and Boarding Pass Verifiable Credentials (VC). For the PoC, temporary schemas were utilized as the IATA standard schemas for both are yet to be developed; this development is scheduled for 2024. Additionally, exploring alternative processes for opt-out options is crucial to align with various privacy laws and regulations across jurisdictions. Future Proof of Concepts will experiment with different opt-out or consent withdrawal processes to ensure compliance and flexibility in handling passenger preferences.

© 2023 International Air Transport Association. All Right Reserved.

Our Partners



International
Air Transport
Association
Route de l'Aéroport
33, P.O. Box 416 1215,
Geneva 15 Airport,
Switzerland.
Tel: +41 (0) 22 770 2525