Fact Sheet

Digital Identity for One ID

This Fact Sheet is to provide an overview of digital identity and its role in facilitating seamless and contactless travel as stated in IATA's One ID Standards and Recommended Practices.

1. WHAT IS DIGITAL IDENTITY

- Digital identity is a set of **electronically** captured and stored **attributes** and **credentials**[1] that can uniquely identify a person.
- For the purpose of **One ID**, digital identity covers the **biographic** and **biometric** information of the passenger, e.g. passport information.

2. TODAY'S PROBLEMS

- In today's air travel journey, passengers have to prove their identity to multiple parties, e.g. airlines, airports and governments, by providing their physical identity document.
- Today's manual identity-checking processes have several challenges:
  - Passengers have to share all the data as written in the identity document even though not all the data will be needed for every transaction.
  - A physical identity document is susceptible to forgery/tampering and can be lost or damaged.
  - There are limited ways of verifying these physical documents.
  - It involves human intervention, which can result in queues and congestion at the airport.
- Passenger traffic is expected to double the 2019 number in 2041, and airports capacity will not be able to keep up with the demand without process improvement through automation and digitalization.

3. DIGITAL IDENTITY AS A SOLUTION

- IATA recommends using a decentralized digital identity, as opposed to a central database or repository.
- Decentralized digital identity enables the holder (the passenger) to fully own and control his/her identity information and directly share this information with relevant parties.
- Minimum level of required information is shared and only upon consent.
- Given that a passenger journey involves various stakeholders who deal with various sets of passenger information, using decentralized digital identity can help strengthen data privacy and protection, through secure communication only between issuers (airlines, airports, governments or third parties) and holders (passengers) and subsequently holders and verifiers (airlines, airports or governments).
- Since there is no centralized database, using a decentralized digital identity can also help reduce cybersecurity risks.
- Data presented online has equivalent or higher trustworthiness than the physical presentation enabling digitalization and simplification of business processes.

4. BENEFITS OF USING DECENTRALIZED DIGITAL IDENTITY

The use of digital identity can bring benefits to all parties by enabling automated processing, and thus improving passenger experience with faster processes and less queues. This will help airlines, airports and governments to save or reallocate their resources. The possible benefits for each stakeholder are as follows:

Stakeholders	Benefits
Passengers	Strengthened privacy protection; Reduced need to show their identity documents multiple times during their journey; Seamless and contactless experience at the airport through automation; Convenient sharing of the identity information as opposed to filling in the data by themselves manually
Airlines	Higher trust in identity document validation; Improved data quality in capturing the Advance Passenger Information (API) that needs to be submitted to States; Coupled with biometrics, greater opportunities to offer their customers a seamless and contactless experience at the airport;
Airports	Higher trust in identity document validation; Stronger privacy protection, through the ability to receive only the minimum required information about the

[1] Credential: A set of one or more claims made by an issuer according to the W3C definition; https://www.w3.org/TR/vc-data-model-2.0/#claims; In the travel context, it can include passport, boarding pass, frequent flyer card, visa, national ID, driver's license, etc.

	passenger that is needed for transactions; Coupled with biometrics, greater opportunities to offer passengers a seamless and contactless experience at the airport by receiving the passenger information in advance prior to departure where applicable;
Governments	Higher trust in identity document validation conducted by airlines or airports; Improved data quality for the API and/or travel authorization applications, where passengers can choose to share digital identity as opposed to filling in the data manually; In the case of using the States-issued digital identity, opportunities to process the passengers in advance prior to their arrival and/or automate the arrival border process;

5. WHAT IS THE ICAO DIGITAL TRAVEL CREDENTIAL (DTC)?

- Travel credentials in a **digital** format that is meant to **substitute a conventional passport** temporarily or permanently with a digital representation of the traveler's identity.
- The DTC is mainly designed to **serve border control purposes.**
- Three **types** of DTCs are envisaged depending on the binding to ePassport. Currently, the technical specifications are available for a DTC type that requires the possession of a physical passport in parallel.

6. FAQ

- **What would be a trusted digital identity that the industry can use?** For air travel, a digital identity issued by a State will be the one most trusted. However, in its absence, a **passenger can self-derive** a digital identity using a third-party application (provided it is considered a trusted issuer). Such a self-derived or a third-party-issued digital identity can be used at non-government-managed touchpoints, e.g., check-in, bag drop, and boarding.
- **Is digital identity a prerequisite for One ID?** To achieve digitalization of admissibility, digital identity will be needed for passengers to demonstrate their possession of the right documents to airlines remotely, digitally, and securely. For contactless travel as well, digital identity will be needed except in a very few cases. If a contactless process is available at a location where all the passengers can go through touchpoints with biometrics recognition without a separate enrolment, e.g. by leveraging the government's database, digital identity may not be needed.
- **Will digital identity fully replace physical travel documents?** No. In the short/medium term, travelers will need to carry physical identity documents (e.g. passports) with them, although they may not need to show these documents at all touchpoints and/or in all cases. However, the vision is to replace physical identity documents with digital identity in the long term.
- **How can the ICAO DTC be used for One ID?** It would be ideal if States issued a DTC to the passenger's device directly. If not, the industry can still create a digital identity by reading the information stored in the ePassport chip to make processes more secure and efficient. The industry can leverage the trust of the DTC or the ePassport and use it for passenger processing.
- **Can using digital identity replace physical travel document checks at different touchpoints in the journey (i.e. check-in, bag drop, boarding)?** It will depend on whether it is allowed legally (regulatory framework). If it is, airlines can then make their own assessment and decide whether to use digital identity to replace physical identity document checks.
- **Airlines are today responsible for document checks at various touchpoints. Will this be changed if an airline uses digital identity?** No. Using digital identity can be more efficient, secure, and privacy-protecting, but it does not mean that the airline's responsibility will be removed . Also, it doesn't mean that airlines should be required to have more responsibility, e.g. authenticating travel documents, just because they might be able to do so by using digital identity. But, IATA will continue to engage governments to adopt more pre-travel verification through direct communication between passengers and governments so that airlines only need to check if a passenger has received clearance from the destination rather than checking travel documents to make that judgement.
- **What One ID standards are available on digital identity?** IATA has so far developed the W3C Verifiable Credentials schema[2] for passport, visa and the ICAO Digital Travel Authorization (DTA).
- **What is the difference between a digital identity and a digital identity wallet?** The digital identity wallet is the 'container' in which digital identity as a set of attributes/credentials will be securely stored on the passenger's device. This wallet could also contain other credentials where applicable, such as visa, frequent flyer info, lounge pass, etc.
- **The EU is now developing standards and recommendations for European Digital Identity. How will this impact IATA One ID?** IATA is closely monitoring it and participating in some of the discussions in an advisory capacity. IATA will endeavor to ensure the alignment of the One ID standards with the EU's digital identity.
- **Some governments have already introduced or are looking at introducing national digital identity. What does it mean to One ID?** If the national digital identity will also be used for cross-border use cases, it should be interoperable with the One ID standards and recommendations. Even if it does not support cross-border use cases, IATA will still be keen to understand the framework, to see if the industry can leverage it in using other party-created digital identities for travel.

[2] As of September 2023, the schema is available as alpha specifications for the industry's testing. Once testing is done and finalized, it will be published on the IATA Developer site.