Fact Sheet

Verifiable Credentials & One ID

This Fact Sheet provides an overview of W3C Verifiable Credentials that support the One ID Standards and Recommended Practices.

1. TODAY'S CHALLENGES

- While traveling, passengers must show their credentials to access entitled services or go through processes.
- Such credentials include booking reference, passport information, visa, frequent flyer membership, etc.
- Especially passport and most of the other documents that passengers need to demonstrate their possession to airlines are in a physical form and thus checks or validation of these documents are manually done.
- Manual checks or validation of the documents can result not only in queues and congestion at the airport but also inconvenience and distressing experiences for passengers.
- Also, when the credentials are in physical forms, there are other challenges as well:
  - They are susceptible to forgery/tampering and can be lost/damaged.
  - Their holders, i.e. passengers, do not control their data and do not have a choice but to disclose all the information on the document that may not be necessarily needed to get services or go through the processes. This poses a privacy risk.
  - Manual checks and validation of the documents cannot ensure whether the credentials are authentic, genuine, or have not been tampered with.

2. WHY AND WHAT IS A VERIFIABLE CREDENTIAL

- The use of a Verifiable Credential (VC) may help address the above challenges.
- A VC is a digital representation of an existing physical credential (e.g. passport, boarding pass, visa).
- Key features of a VC are:
  - It is digitally signed to demonstrate authenticity and integrity.
  - It is stored in a digital wallet.
  - It contains general info (type of credential, issuer), claims, and digital signature.
  - It may support privacy-enhancing technologies, such as selective disclosure, and zero-knowledge proofs.
- VCs can also be derived. In the travel use cases, VCs can be created using an existing authority-issued identity or travel document such as a passport.

3. VERIFIABLE CREDENTIALS ECOSYSTEM[1]

- **Issuer**: digitally signs the credentials and sends them to the holder (e.g passport office, IATA, or any other trusted 3rd parties)
- **Holder**: possesses the credential and presents it to the verifier as proof of claims (e.g. traveler, travel agency)
- **Verifier**: makes sure a trusted issuer issued the credentials and verifies that the claims are valid (e.g. airline, airport, government)

4. VERIFIABLE CREDENTIALS STANDARDS

- According to the guidance from the IATA Digital Transformation Advisory Council[2], all the industry digital identity programs IATA manages should leverage the existing open technology standards such as Decentralized Identifier (DIDs) and Verifiable Credentials from W3C.
- The World Wide Web Consortium (W3C) develops standards and guidelines to help everyone build web-based digital identity solutions on the principles of accessibility, internationalization, privacy, and security.
- The W3C Verifiable Credentials support digital identity programs for State and industry actors alike.

5. BENEFITS OF USING W3C VERIFIABLE CREDENTIALS

- Helping achieve global interoperability as:
  - they are based on open standards;
  - there is no direct relationship required between the issuer and the verifier for verification; and
  - they are persistent and reusable for future travels and other purposes beyond travel.
- Ensuring data protection due to:
  - verifiable personal data can be presented by the subject to the right actor at the right time removing the need for a trusted commercial and operational system to store and forward personal information; and
  - only the minimum data required to be exchanged without losing trustworthiness, i.e. selective disclosure

[1] https://www.w3.org/TR/vc-data-model-2.0/#ecosystem-overview

[2] https://www.iata.org/en/about/corporate-structure/dtac/

6. VERIFIABLE CREDENTIALS AND ONE ID

- Airlines are required to ensure that passengers hold the right travel documents for transit and entry into a country (e.g. passport, visa). Such documents are normally paper-based, requiring manual checks at the airport.
- One ID aims to digitalize the airline's document-checking process using digital identity and VCs. The IATA Recommended Practice 1701p Digitalization of Admissibility provides the description of the end-state for this process. Where possible, passengers can store their passport and other travel documents as VCs in their wallet and digitally demonstrate their possession of the documents to airlines before departure.
- To support this RP, the W3C VC schema for travel and other documents is necessary. Therefore, IATA has developed alpha specifications for VC schema for passport, visa and the ICAO Digital Travel Authorization (DTA)[3]. They are available for industry testing[4] and will be available for the public once finalized. The alpha specifications are yet to fully support selective disclosure nor zero-knowledge proof, but IATA will work towards making those features available in the near future.

[3] ICAO Digital Travel Authorization (DTA) https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Digital%20Travel%20Authorizations.%20%28New%29.pdf

[4] As of December 2023