One ID End State and Key Principles

This paper should be read in conjunction with the One ID Concept Paper (Version 1) and aims to clarify the One ID desired End State and key principles as set out by the One ID Advisory Group.

The Current State and Why It Isn't Sustainable

As described in the One ID Concept Paper, today's reality is that the combination of increasing passenger numbers, limited physical infrastructure, enhanced security requirements and legacy processes result in more friction and a complicated, unpleasant experience for passengers.

Current infrastructure is incapable of supporting forecasted growth without finding innovative methods and processes to support this growth. In many locations, expansion is simply not an option due to space limitations, and where expansion is possible it may not be accomplished in a timely manner due to lengthy planning processes and will require significant capital expenditure. A more efficient use of current infrastructure, leveraging innovative methods and processes, will help to avoid or delay these issues.

Desired End State

The One ID program will develop a roadmap describing the current state and demonstrate a clear trajectory to the desired end state via several interim states that describe the actions that can be taken and the solutions that can be deployed in the near and medium term.
In terms of a time horizon, the desired end state for One ID coincides with IATA's NEXTT (New Experience in Travel and Technology) vision, i.e. 2035. We are aiming to describe what we envision the end-to-end passenger process to look like in 2035, where it relates to elements of identity management that are in scope of One ID. In order to avoid becoming too prescriptive in terms of specific solutions or deployment options, we describe the desired end state by its key principles. We also document a series of assumptions underpinning the key principles that describe the desired end state.

Key principles describing the desired end state

- The various public and private stakeholders that interact with the passenger across the end-to-end journey collaborate with one another towards a unified, passenger-centric approach.
- The passenger is made aware that his/her data are being collected, for what purpose, and to provide consent where necessary, all in line with applicable regulations.
- Passenger identity information[1] is captured and verified as early as possible in the process (at the time of booking or shortly thereafter), which will allow control authorities to perform more robust advance risk analysis and keep inadmissible passengers off the airline, while allowing the airline to offer a more tailored experience and handle exceptions earlier on.
- The majority of passengers arrive at the airport "ready to fly". The legacy terminology "check-in" will disappear in favor of "ready to fly" which includes several of the constituent elements of the check-in process and more, such as:
  - The passenger has "confirmed" or "standby" status for the flight and, if confirmed, has assigned seating.
  - Where applicable, the passenger's identity has been authenticated [is this passenger who (s)he says (s)he is].
  - Where applicable, the identity document/credential has been authenticated [is the credential valid, genuine and not been tampered with].
  - The passenger's admissibility has been validated [is the passenger authorized to travel to destination].
  - The passenger is biometrically enrolled such that (s)he can be biometrically verified at subsequent touchpoints. This enrollment would persist across multiple trips, or be replaced by a persistent government-issued digital travel credential.

[1] Advance passenger information that includes certain attributes that will allow an organization to recognize an individual. In today's world it is API but may include additional attributes, such as biometric information, in the future.

- The passenger uses his/her biometric(s) as a single token at all touchpoints across the end-to-end journey, including departure, transfers and arrivals, and where possible including the return trip. This should include, but is not limited to, bag drop, secure area access, security screening, outbound border control, lounge access, boarding, inbound border control. It assumes that all these touchpoints are biometrically enabled to verify the passenger's identity, where possible without breaking stride.
- Physical touchpoints and processes are combined, removed or moved off-airport to the greatest extent possible, in order to achieve a truly seamless ground process. For instance, outbound border control could be integrated into the security access or boarding process.
- Passenger information is shared in advance of the passenger journey and is shared with the different public and private stakeholders who interact with the passenger across the journey (departure, transfers and arrival).
- Public and private stakeholders that interact with the passenger across the journey can access relevant elements of the information on an authorized-to-know basis and in compliance with applicable privacy and data protection regulations, allowing them to perform advance processing and analysis in order to facilitate the passenger process.
- Hold baggage is linked to the passenger identity.
- Systems and data formats are interoperable across different airports, airlines and States.
- The majority of passengers move through various airport touchpoints, including border control processes, with minimal disruption and ideally at walking pace (departure, transfer and arrival).
- One ID facilitates the sharing of the passenger's biographical, biometric and travel document information between the various public and private stakeholders that interact with the passengers across the journey and have a valid reason (need-to-know / authorized-to-know) to access certain data in order to process passengers correctly, safely and securely. This is the "core" of One ID.
- Benefits could be derived from sharing flight data and process information (such as touchpoints passed, time stamps, flags/signals, record of exceptions, etc.); this would be considered "non-core" but can help to deliver optimal service to passengers.
- Public and private stakeholders who interact with the passenger across the journey, experience improved productivity, capacity and cost savings.
- Further reduce human trafficking and other cross-border criminal activities due to reduced possibilities for individuals to cross borders under false identity.
- Risk-based differentiated screening, both for border and aviation security processes, will be facilitated.
- One ID will not introduce any additional steps or process to the existing passenger process.

Assumptions surrounding or underpinning the key principles

- The principles apply to various travel scenarios, international and domestic, including connections/transfers travel. They will be developed with the intention to apply such principles to the broader Travel and Tourism industry, not restricted to air travel only.
- There will be agreements and operational frameworks governing collaboration between stakeholders. Operational frameworks can exist for a local air travel ecosystem and at national/international levels. Regulatory changes will accommodate this.
- A trusted, digital identity will enable off-airport identify information validation.
- To cover nearly 100% of travelers in various travel scenarios, a multi-modal approach to the digital identity will probably be required – including for instance the ICAO Digital Travel Credential (DTC) that is an evolution of the e-passport, but equally other identity schemes including government-run Identity-as-a-Service schemes, national identity schemes, as well as private sector initiatives.
- To the extent possible, biometric enrollment (capture of the biometric for a later use) is persistent across multiple trips and for a reasonable period of time.
- Biometric recognition is used for identity verification throughout the various process steps, removing the need to physically present travel documents and/or credentials at every touchpoint.

- The use of biometrics should be multimodal, i.e. one stakeholder could be using one type of biometrics while other stakeholders could be using other, and, these should be interoperable.
- ICAO approved biometrics, allowing for 'on the move' recognition are to be used (for example: face, iris and fingerprint).
- To be trusted by other stakeholders in subsequent process steps including cross-border scenarios, identity authentication will most likely be performed, or supervised, by a government agency against a government issued travel credential.
- There is a need for a systems infrastructure that enables identity management collaboration, i.e. an environment where different stakeholders can share, use and amend passenger information throughout the journey (i.e. the identity management platform in the broad sense of the term). Interoperability between disparate systems in different locations will be critical.
- The "ownership" of the identity management systems infrastructure will differ from location to location; it could be a single stakeholder such as a government agency, or it could be joint "ownership" governed by an operational trust framework.
- Privacy by Design principles apply.
- Privacy and data protection regulations are strictly adhered to.
- Passenger consent to disclose additional information (i.e. biometrics data) will be sought where/when applicable.
- There should be a clear distinction, in terms of getting passenger consent, between core identity management functionality(ies) versus non-core functionality(ies) related to process efficiencies, commercial or marketing purposes.
- The legacy check-in process will not exist in its current form.