Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific **Prosperity**

Achieving Harmonization of a Biometric ID Management Framework across APEC Economies: Practical Guidebook and Roadmap

APEC Digital Economy Steering Group

May 2023

Achieving Harmonization of a Biometric ID Management Framework across APEC Economies: Practical Guidebook and Roadmap

APEC Digital Economy Steering Group

May 2023

APEC Project: DESG 03 2021A

Produced by

Thomas D. Pellegrin, Senior Principal, IATA Consulting
Lian Zhang, Principal, IATA Consulting
Li Yuan Soh, Consultant, IATA Consulting
Email: consulting@iata.org

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#223-CT-03.3

Contents

1. Introduction

1.1 Biometrics in aviation

Biometric technology in air transport has seen significant adoption in the past twenty years. More recently, airlines, airports, and authorities have recognized the benefits of removing physical touchpoints at airports to increase traveler confidence related to the COVID-19 transmission risk. As a result, the speed of adoption and extent of buy-in from stakeholders have increased.

However, biometric implementations in aviation often see individual stakeholders, such as airlines, airports, and border control agencies, designing their biometric-enabled processes to suit their own operational and statutory requirements. This results in travelers having to register their biometric features multiple times or alternate between presenting their travel documents, such as boarding passes, and verifying themselves biometrically across different touchpoints throughout the cross-border journey.

For a fully biometric-enabled traveler journey at the airports, the different stakeholders within and outside their economy or territory need to be aligned on a common vision for biometric implementations in cross-border air travel.

1.2 About the project

To assist APEC economies with improved cooperation and a shared Biometric ID vision and roadmap, APEC launched a project that aims to:

I. Learn from global implementations to drive the success of Biometric ID within APEC economies,

II. Raise awareness and obtain support for the Biometric ID process among APEC economies, and

III. Provide practical guidelines on Biometric ID adoption for harmonization across all APEC economies. The present document provides those guidelines.

1.3 About this guidebook

The guidebook is proposed as a reference for APEC economies planning, implementing, or expanding the use of biometric identification solutions in cross-border travel. This guidebook sets a recommended end-state vision and includes implementation stages and key success factors for consideration. However, implementations by different stakeholders and in different economies will also depend on unique factors that are context-specific, such as public acceptance of the biometric ID concept, and existing policies, laws, and regulations governing biometric use and data collection.

This guidebook is developed with supporting insights from:

- The Global Benchmarking Study, issued as a separate document,
- Survey conducted from August to October 2022 with 44 stakeholders from 22 different economies, including airport operators, airlines, associations, border control agencies, civil aviation authorities, and other relevant authorities,
- Ten stakeholder interviews with airport operators, authorities, and biometric identification solution providers, and
- Internal and external publications or reports on biometric identification technologies in general and specific to the aviation sector.

2. Biometric ID management framework

The purpose of this section is to propose a framework for APEC economies to plan for harmonized biometric implementations in cross-border air travel. The framework described in the present section comprises a common taxonomy of key concepts and a recommended vision for end-state and interim-state implementations consistent with emerging and established standards, recommended practices, and technical specifications from international organizations (such as ACI, IATA, ICAO, and ISO). The section after this one contains practical implementation guidance.

2.1 Definitions

This section proposes a taxonomy of terms frequently used in the framework to establish a mutual understanding among the APEC economies.

2.1.1 Admissibility

In the context of this guidebook, **admissibility** refers to the ability of the traveler to enter controlled-entry areas throughout their journey. These include:

- **Outbound airport terminal:** the airport grants the traveler permission to enter the landside (where applicable) or airside area of the terminal. That permission is typically based on the traveler providing a valid travel document, such as an airline ticket (at the landside entrance) or a boarding pass (at the airside entrance)[1]. The issuance of the boarding pass by the airline is itself contingent on the traveler proving their identity, ownership of a valid ticket, and right to enter the destination state based on citizenship or holding the appropriate entry permit.

- **Outbound border crossing:** the state government of the traveler's place of origin grants the traveler permission to leave the state. That permission is typically based on the traveler providing a valid identity document, and any associated entry permit to demonstrate compliance with the overstay rules.

[1] Note as an example that biometrics are already widely used to ascertain the airside admissibility of airport staff at airports worldwide.

- **Lounge:** the lounge operator grants the traveler permission to enter its facilities based on the traveler providing a boarding pass of the right travel class, or evidence of membership into the appropriate loyalty or lounge program.

- **Aircraft:** the airline grants the traveler permission to board a flight from a boarding gate, typically based on the traveler providing a valid boarding pass and (optionally) a travel document, such as an identity document.

- **Transit airport terminal:** the airport grants the traveler permission to enter and stay within the transit area in return for the traveler providing evidence that they have an onward flight connection (e.g., an airline ticket or boarding pass) and will not be entering the transit airport's state.

- **Inbound border crossing:** the state government of the traveler's destination grants permission to the traveler to enter the state (e.g., after verification of travel documents, entry permits, health certificates, etc.). This may be done entirely on arrival, or preemptively by verifying the traveler's admissibility ahead of their arrival through Advance Passenger Information (API) data sharing by the airline.

2.1.2 Biometrics

In the context of the present study, **biometrics** refer to the measuring of a wide range of physical characteristics (and, occasionally, behavioral ones) that are unique to every individual (such as fingerprints, the iris of the eyes, scent, gait, or even keystroke dynamics and muscle memory recall) to positively ascertain that individual's identity.

Biometrics constitute one of the three common factors of authentication: what a person **is**, in contrast to what a person **knows** (e.g., the combination to a safe) or **possesses** (e.g., the key to a safe). Among those factors, biometrics stand out for being unique to their owner, impractical to fake, and not relying on the individual's fallible memory and preparedness.

Biometrics are indissociable from technology, which includes hardware sensors to capture a **biometric sample** and related software to parse and match it against a reference.

2.1.3 Biometric sample

In the context of this guidebook, and congruent with ISO/IEC 30108-1:2015, a **biometric sample** is an analogue or digital representation of biometric characteristics prior to biometric feature extraction.

A biometric sample can be full (e.g., a photo of someone's face) or partial (e.g., a mathematical representation of the key characteristics of someone's face, such as the skin tone and interpupil distance). It can also be two- or three-dimensional, depending on the method of capture.

2.1.4 Credentials

In the context of this guidebook, **credentials** are documents in paper or digital form that are used to verify a traveler's admissibility, identity, or both.

- **Admissibility credentials** refer to documents that ascertain a traveler's **admissibility** into controlled-entry areas throughout their journey (as defined above).
- **Identity credentials** refer to a document that establishes **identity assurance**.

A credential can be both an admissibility and an identity credential at once. For example, an identity document serves to establish identity assurance of its bearer, but also verifies the traveler's admissibility into economies that do not require an entry permit for holders of that identity document (including the traveler's own economy).

Ideally, digital credentials that are not single-use (e.g., identity document and health certificates, but not airline tickets nor boarding passes) should persist until their date of expiry, so that travelers can reuse them in multiple journeys without the need to create them again.

Table 1 provides common examples of admissibility and identity credentials.

Table 1: Examples of admissibility and identity credentials

Issuer and credential	Admissibility	Identity
Airline		
Program membership	●	
API	●	
Ticket	●	
Boarding pass	●	
State of citizenship, residence, origin, or destination		
Identity document	●	●
Entry permit	●	
Notice of admissibility	●	
Health authorities		
Vaccination certificate	●	
Traveler		
Biometric sample		●
Arrival declaration form	●	

Credentials can exist in either digital or physical form. They are further said to be **digitally verifiable** when they are not only paperless, but also:

- **Cryptographically signed** by the issuer as proof of authenticity (i.e., no one else could have issued them) and integrity (i.e., they were not tampered with); and,

- **Reconcilable** by a verifier against a data registry to check their status (e.g., not expired nor revoked). Note that the reconciliation does not necessarily require read access to the registry in question; the verifier can send a status check request to the owner of the registry, who returns a positive, negative, or no-match result.

Such digitally-verifiable credentials may be issued to a traveler's **digital wallet** by an airline, government authority, or any other authorized third-party involved in the traveler's journey. The Apple Wallet that stores digital boarding passes onto mobile phones is example of a digital wallet that is not travel-specific. IATA is developing and will be releasing a recommended standard on the data structure of digitally-verifiable credentials.

Additionally, digitally-verifiable credentials may be **derived** from credentials issued in a non-digital or non-digitally-verifiable format using a third-party application. For example, a traveler enrolling into a biometric program (such as Star Alliance's) can take a picture of their physical identity document's main page for the mobile app to verify the traveler's identity and issue a digitally-verifiable token. Only that digitally-verifiable token is then required for future interactions of the traveler and the program administrator.

2.1.5 Digital wallet

A **digital wallet** is a self-custodial application that securely stores digitally-verifiable credentials in a format such that the holder of the digital wallet can **selectively disclose** required data to any verifying party (e.g., to an airline to prove travel admissibility to a destination).

The digital wallet should support the following functions:

- Receive and store issued digitally-verifiable credentials, such as those in Table 1, either by receiving them electronically from a third party, or by uploading them locally (e.g., by scanning a travel document using the mobile phone camera or NFC reader).
- Share digitally-verifiable credentials for the purpose of admissibility and identity verification, and only with the full consent of the wallet owner.

The traveler's custody of their full set of admissibility and identity credentials, as permitted by the digital wallet, is a key aspect of the **self-sovereign identity** concept.

2.1.6 Digital identity

Digital identity refers to a digital representation of a traveler's identity that is provably theirs, such as that provided by identity credentials contained in digital wallet.

In the context of this guidebook, the process of creating a digital identity is referred to as **onboarding** and is occasionally referred to as **enrolment** in the literature. The purpose of onboarding is to **reconcile** (sometimes referred to as **merge**) a traveler's identity credential (such as an identity document) with their biometric sample (such as their face). To that end, onboarding must provide the following features:

- Authentication and validity verification of the traveler's identity credential, which is typically scanned into the digital wallet using the mobile phone camera or NFC reader, either locally or using a secure remote authentication service. Users of mobile banking-related applications may be familiar with this onboarding step as part of the "Know Your Customer" (KYC) checks.

- Biometric presentation attack detection (congruent with ISO/IEC 30107-4:2020), which consists in capturing a biometric sample from the traveler (typically, their face using the mobile phone camera) and using liveness detection techniques to thwart attempts at identity spoofing. For example, the app may require that the traveler rotates their head slightly along the left-right and up-down axis to rule out two-dimensional pictures being presented to the camera.

- Biometric claim verification, which consists of verifying the traveler's assertion that they are indeed the source of the biometric reference contained in the identity credential. This is done by reconciling their captured biometric sample with the biometric reference using software matching.

The outcome of onboarding is the creation of the traveler's **digital identity** that can then be used for identity assurance during the traveler's journey.

2.1.7 Identity assurance

In the context of this guidebook, and congruent with ISO/IEC 30108-1:2015, **identity assurance** is the process of establishing, determining, and/or confirming a traveler's identity. For example, capturing a traveler's **biometric sample** at the airport and reconciling it with the **digital identity** contained in their wallet proves that they are the rightful owner of the identity credentials associated with that digital identity.

2.1.8 Seamless journey

In the context of this guidebook, the **seamless** (or frictionless) journey is the concept of walking-pace processing throughout the airport, leveraging biometrics to remove the need for the traveler to stop, queue, and hand over physical credentials at any checkpoint.

The concept is related, but not identical to that of the contactless journey. The seamless journey should use contactless technology, such as facial recognition, to enable walking-pace processing. Contactless technologies also bring added benefits of enhanced sanitary conditions.

Core to the concept of the seamless journey is that of "**ready to fly**", which consists of the verification of the traveler's admissibility credentials before they arrive at the airport. What is then left to do at the airport itself is to perform biometric **identity assurance** on the traveler.

2.1.9 Self-sovereign identity

In the context of this guidebook, self-sovereign identity refers to the exclusive control that a traveler has over their identity credentials. It is adjacent to, and compatible with the "privacy by default" concept in that the traveler chooses when and whom to share their details with, based on informed consent and a need-to-know basis.

To be self-sovereign, the traveler's digital identity must satisfy the following requirements.

- The traveler should always be in control of when and to whom their admissibility and identity credentials contained in their digital wallet are shared, following a principle of **selective disclosure**. This implies that the traveler should also have the option to disclose part of a credential that is relevant to the journey step, and not others. Conversely, the verifiers should be requesting only the minimal set of data that they need to effectively check the admissibility or identity of the traveler on a **need-to-know basis**, and nothing more.
    - In practice, this requires that the traveler is transparently informed of which stakeholder is requesting the data, the nature of the admissibility and identity data being requested, and the purpose for which the data is being requested. For example, the airport staff operating a security checkpoint may ask the travelers to disclose their boarding pass from their digital wallet for the purpose of reconciling it with their biometric sample (such as their facial image) to grant the traveler access to the airside area of the terminal.
- A corollary to the selective disclosure principle is that the traveler should always retain the ability to **opt out** of sharing their digital credentials and fall back to a manual, non-biometric mode of admissibility and identity verification using paper-

based credentials. That degraded mode will also accommodate travelers who do not own a mobile device and digital wallet.

- Furthermore, the traveler should retain the ability to always update and delete data from their digital wallet, consistent with the concept of having full self-custody.

2.2 A vision for the end state

The purpose of this section is to propose a vision for the end state of cross-border biometric implementations that is consistent with the current state-of-the-art standards, recommended practices and technical specifications as issued by organizations such as ACI, IATA, ICAO, and ISO. This proposed vision was articulated after a thorough review of both SARPs and thought leadership available publicly and privately through industry working groups, as well as subject matter interviews and consultations. This vision is not intended to be prescriptive, but rather to form guidance for APEC economies to converge toward a common end state of cross-border biometric implementations.

> The proposed vision for the end state in cross-border air travel consists of a **seamless** and **contactless** biometric-enabled traveler journey from departure to arrival and back, which requires full **interoperability** between APEC stakeholders across borders. The vision relies upon the concept of **self-sovereign digital identity** in which **admissibility credentials** are checked prior to reporting at the airport ("ready to fly") and only **identity credentials** are verified at the airport.

2.2.1 Key elements of the vision

2.2.1.1 Seamlessness

The proposed end state fully embraces the seamlessness concept, by which the traveler's biometric samples are reconciled at a walking pace with their digital identity. Seamlessness can be achieved without the use of biometrics, but is greatly enhanced by them and by the early verification of the traveler's admissibility into the origin airport, on board the aircraft, and out of the destination airport prior to the traveler reporting to the origin airport for the start of their journey (the "ready to fly" concept). Stated differently, the traveler is known to be admissible before they arrive at the airport, and all there is left to do inside the terminal is to confirm that they are who they claim to be by reconciling their biometric sample with the biometric reference that forms part of their wallet's digital identity.

True seamlessness will further enable APEC economies to exceed ICAO's Annex 9 recommended goal of no more than 60 minutes for departure/outbound processing, and no more than 45 minutes for arrival/inbound processing. Benefits include an improved traveler experience and more dwell time in the retail and food & beverage (F&B) areas of the terminal, which has the potential to increase non-aeronautical revenue for airports.

⚠ We acknowledge that the truly seamless journey is a long-term aspiration that is challenging to achieve. In the interim, APEC economies should consider gradually reducing the number of touchpoints at the airport, introducing biometric-assisted automation at each touchpoint, and verifying the admissibility of travelers in advance to get travelers ready to fly as much as is practical. This could be done, for example, through:

- Direct communication between passengers and authorities to collect the required admissibility information. This way, a single notification of approval to travel can be issued instead of multiple authorizations. The number of documents that airlines are required to check at check-in is thus minimized, or
- In cases where economies have interactive Advance Passenger Information (iAPI)[2] in place, they may consider linking the notification of approval with iAPI, so that airlines can rely on only the iAPI response (without the need to check the documents) to completely automate the check-in process.

[2] ICAO Annex 9 defines iAPI as an "electronic system that transmits, during check-in, API data elements collected by the aircraft operator to public authorities who, within existing business processing times for passenger check-in, return to the operator a response message for each passenger and/or crew member".

2.2.1.2 Contactlessness

In the end state, the technology used to capture biometric samples from travelers should not require physical contact. While the speed benefit of contactless technology (such as facial capture) is not necessarily significant relative to contact technology (such as fingerprint detection), the COVID-19 pandemic has evidenced the importance of eliminating touch surfaces to combat disease spread and reassure travelers. In that sense, contactless technology provides an added layer of resilience to the industry and a risk mitigation factor in future pandemics.

> ⚠ We acknowledge that biometric technology convergence is a long-term aspiration, because APEC economies may disagree on technical orientations and standards, or may have committed to technology investments that will require full amortization before they can be changed. In an interim state, what matters more is the interoperability of systems, even if it initially requires that travelers submit more than one type of biometric sample. Likewise, those APEC economies that have opted for contact technology (such as fingerprint or palmprint) should aim to have them frequently and visibly sanitized.

2.2.1.3 Paperlessness

In the end state, the pre-travel admissibility is verified entirely digitally and remotely, and the on-airport identity verification is performed using no other means than the reconciliation of a captured biometric sample with a biometric reference contained in the traveler’s digital wallet.

This process assumes the digitization of all paper-based credentials. While the air transport industry has been mostly successful at eliminating paper tickets, boarding passes and entry permits remain in a mix of physical and digital forms, and identity documents are still mostly paper-based.

Regardless of progress in digitization of travel credentials, the end state should always allow for a degraded mode of verifying travelers’ admissibility and identity that relies on paper credentials, both to mitigate the risk of systems downtime and accommodate those travelers who cannot or will not use a digital wallet.

⚠ We acknowledge that eliminating all paper credentials and replacing them with digital equivalents is an ambitious component of the end-state vision. Getting governments to mutually recognize identity documents in full digital form for border control purposes is especially challenging. Bilateral agreements among APEC economies can gradually make this end-state vision a reality by trialing it on select intra-APEC routes.

2.2.1.4 Interoperability

The end-state vision for biometric implementation in cross-border air travel is one where both processes and systems should be fully interoperable between all stakeholders to provide a consistent and predictable experience to the traveler.

Interoperability does not mean nor require that all APEC economies follow the same process nor select the same technology and systems, but rather that there is a mutual recognition of each other's process and technology to eliminate inconsistencies and gaps in the traveler's journey.

Interoperability means that the credentials and biometric references provided by the travelers should be compatible across three levels of stakeholders:

- Within an airport (e.g., airline, airport operator, border control agencies),
- Between different airlines and airports within an APEC economy (domestic travel), including those under multiple ownership, and
- Across airlines and airports in different APEC economies (regional travel).

To enable greater interoperability across stakeholders, airports, and the economies, APEC economies should adopt open standards (e.g., ICAO DTC and ISO standards), rather than develop and use closed standards.

For example, the European Union (EU) establishes EU-wide regulations under a framework for a European Digital Identity[3] for secure public electronic identification.

⚠ We acknowledge that full interoperability across all 21 APEC economies is a long-term goal. In the interim, we recommend that economies with similar levels of biometric adoption and maturity, and with similar ambitions for inducing traffic through travel experience innovation, work together at process and system compatibility and harmonization in small peer groups. Their work will eventually lead the way and provide a blueprint for other APEC economies that are further behind in their biometric adoption and maturity.

[3] COM(2021) 281 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

2.2.1.5 Self-sovereign digital identity

In the vision for the end state, the traveler should exclusively own their digital wallet and have custody of all information contained within it. Consent should be sought and obtained whenever data from the traveler's digital wallet is requested by a third party for a specified purpose related to the traveler's journey. The traveler should be allowed to opt out of using their digital identity at any time and revert to a paper-based admissibility and identity verification process.

> We acknowledge that the concepts of self-sovereign identity and self-custody digital wallet are contingent on a high degree of technological literacy and mobile device ownership among the traveling population. In the interim state of the cross-border biometric implementation, APEC economies may consider custodial services provided by a third party, while ensuring that the key privacy concept of selective disclosure remains enforced. The third party may, with the consent of the traveler, collect and share with other verifying parties (e.g., border authorities), the required credentials for admissibility and identity verification.

2.2.1.6 Persistence of credentials

In the proposed vision for the end state, the traveler should be able to reuse the same set of digitally-verifiable credentials on multiple trips, until the credential itself is deemed invalid (e.g., the identity document has expired or was revoked). This is a step change from the current mechanism of per-trip enrolment that prevails in several of the biometric implementations that exist today.

Each type of credential has its own natural validity period, as illustrated in the table below. While certain credentials (e.g., flight ticket) are only valid for a single trip, other credentials like identity credentials are valid for a longer duration and should be able to be used without the need for multiple registrations or creation in the digital wallet, e.g., before every trip.

Table 2: Typical validity periods of various admissibility and identity credentials (illustrative)

Issuer and credential	Use	Typical validity period
Airline		
Program membership	Persistent	Lifetime
API	Single	Single leg
Ticket	Single	Single trip (incl. return)
Boarding pass	Single	Single leg
State of citizenship, residence, origin, or destination		
Identity document	Persistent	5–10 years
Entry permit	Single or persistent	7 days–5 years
Notice of admissibility	Single	Single leg
Health authorities		
Vaccination certificate	Persistent	270 days (e.g., COVID-19) Lifetime (e.g., malaria, yellow fever)
Traveler		
Biometric sample	Persistent	Years (depending on regulations)
Arrival declaration form	Single	Single trip

2.2.2 How the vision works in practice

This section describes how the end-state vision works in practice. As shown in the figure below, there are two types of credentials introduced earlier (admissibility and identity), and each one is subject to separate creation and verification steps. Each one is covered hereafter.

Table 3: Structure of the present section

	Admissibility	**Identity**
Creation	**Creation of admissibility credentials** **(Issuance into the digital wallet)** Section 2.2.2.2	**Creation of identity credentials** **(Digital identity onboarding / enrolment)** Section 2.2.2.1
Verification	**Verification of admissibility** **(Getting the traveler ready to fly)** Section 2.2.2.3	**Verification of identity** **(Biometric reconciliation at the airport)** Section 2.2.2.4

2.2.2.1 Creation of identity credentials

In the end-state vision, the traveler's admissibility at each step of their journey is verified prior to their reporting at the departure airport, and their identity is then reconciled biometrically at the terminal. A digital identity onboarding step is required to enable this process. This digital identity onboarding service allows a traveler to create a digital identity once for any number of trips using a digital wallet mobile app. A non-travel example of a digital identity wallet among APEC economies is Singapore's Singpass app, which allows citizens and residents to create their digital identity on their mobile phones and use it to authenticate themselves with a variety of online services. That example is described in further detail later in this section.

ICAO currently considers three types of biometrics: facial, fingerprint, and iris recognition, and has published SARPs on all three for use in travel documents. Facial recognition, the only mandatory biometric in the travel document (picture), is the most widely used biometric technology in airport processing and is also the biometric recognition method recommended by ICAO. Given its prevalence and contactless nature, facial biometrics (2D or 3D) are a natural candidate for the end-state vision.

Another practical consideration relates to the sensitivity of the traveler's biometric information. To mitigate the risk of the full biometric sample (e.g., the traveler's facial picture) being leaked, a **biometric template** can be used instead. As defined by ICAO, biometric templates are machine-encoded representations of a biometric trait created by a computer software algorithm. A biometric template can be compared against other collected templates during biometric identity verification. Biometric templates create anonymity in data storage and transaction as it prevents image reconstruction in case of a security breach. They are identified as optional "additional biometric security" in ICAO Doc 9303. For example, a biometric template may record the inter-pupil distance on the traveler's face, as well as several other key dimensions, for later reconciliation with the biometric sample captured live from the traveler. In that sense, the biometric template is functionally similar to a mathematical one-way function, such as a SHA-256 hash: the facial picture can be converted to a template, but the template cannot be converted back into a facial picture.

APEC economies should consider using biometric templates, rather than full biometric references, to provide greater privacy protection to travelers sharing their biometrics.

A further related consideration is the proliferation of options for capturing any given biometric trait. While standards for fingerprint biometrics exist, standardized facial and iris biometric templates have not been agreed on, and many facial biometric templates are currently unique and proprietary to each biometric capture technology vendor. The present heterogeneity in facial biometric templates can become a hurdle to interoperability across stakeholders, airports, and economies. For example, the number of dimensions for facial reference and sample capture (i.e., 2D or 3D) in facial recognition varies by stakeholder and implementation today.

Whatever biometric technology and templates APEC economies settle on, they need to be interoperable across stakeholders, airports, and economies.

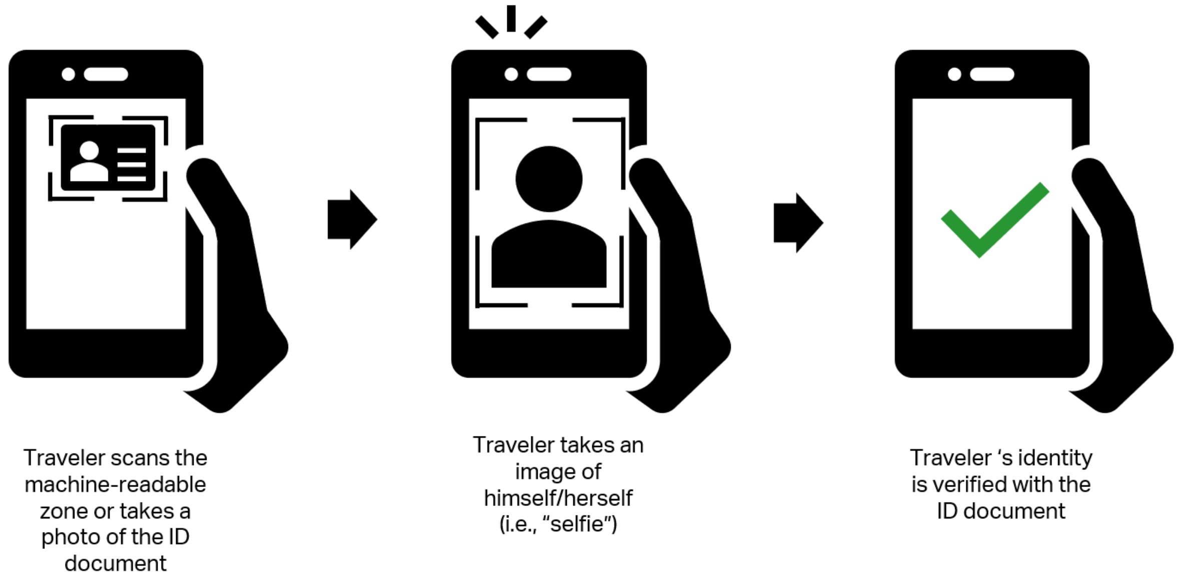
During the onboarding, a traveler will typically create their digital identity by capturing their biometric sample and reconciling it with a suitable identity credential. The traveler first captures their biometric sample (e.g., take a "selfie") from within the digital wallet app using their mobile phone camera. The app performs real-time checks to ensure that the picture is of adequate quality (lighting, face size, etc.), and liveness detection to ensure that the traveler is not spoofing their identity by taking a picture of a photograph instead. Then, the traveler is invited by the app to supply the biometric reference against which to reconcile the sample. That biometric reference is held in an identity document. The traveler may, for example, scan the machine-readable zone contained at the bottom of their biometric identity document's[4] main page, and then scan the biometric chip embedded in the cover of their biometric identity document to unlock the biometric reference stored inside (typically a copy of the biometric identity document picture). The biometric sample and reference are then matched by the app locally, or by remotely contacting a third-party reconciliation service.

Some jurisdictions restrict the use of the biometric reference stored in the identity document (e.g., the photo stored in the identity document's chip) for specific purposes. While the digital wallet ends up storing the traveler's biometric reference at the end of the onboarding process, that biometric reference is a copy of that found in the identity document and may therefore be subject to such restrictions.

APEC economies should conduct a check of the prevailing laws and regulations pertaining to the use of biometric references, in particular those associated with identity documents, and harmonize those where practical to facilitate downstream interoperability of the biometric processes and systems.

[4] **Such biometric identity documents contain a contactless integrated circuit (i.e. chip) that allows the document to securely store the holder's biometric and biographic data.**

Figure 1: Simplified onboarding process, for illustration


Traveler scans the machine-readable zone or takes a photo of the ID document
Traveler takes an image of himself/herself (i.e., "selfie")
Traveler 's identity is verified with the ID document

Onboarding example in a non-travel setting

Singpass is a trusted digital identity for Singapore citizens and residents. This identity is also available on a mobile app, where users can access government digital services using their biometric (e.g., fingerprint or face) or passcode, digitally sign documents, or view notifications from government agencies. Through Singpass, users may also share their details from government sources with organizations without the need to bring or present physical documents.

Singapore's National Certification Authority (NCA) is responsible for both the issuance and management of the trusted digital certificates of individuals and companies. Digital certificates are stored in the user's Singpass application.

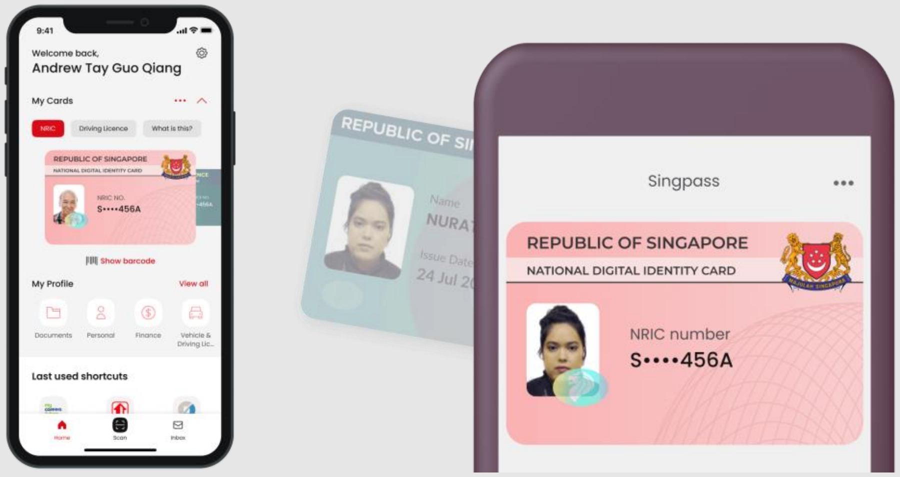


Figure 2: Singpass, the digital trusted identity of citizens and residents of Singapore has a mobile application that allows users to access and share their information remotely without the need for physical documents.

2.2.2.2 Creation of admissibility credentials

In the proposed end-state vision, admissibility credentials (as defined in Section 2.1.4) are those used to verify the traveler's admissibility at every step of their journey prior to their reporting at the departure airport, so that the traveler arrives at the airport "ready to fly". To enable that vision, admissibility credentials must first be created in or issued to the traveler's digital wallet, so that they can later be shared with the relevant verifiers, including:

- Airlines (e.g., ticket, boarding pass), and
- State authorities, such as
    - Border authorities (e.g., notice of admissibility into the destination)
    - Health authorities (e.g., vaccination certificate) and
    - Immigration authorities (e.g., work entry permit).

These credentials should be cryptographically signed and digitally verifiable to prove their authenticity and the traveler's ownership of them. They should be stored in the traveler's digital wallet for a validity period that is specific to the credential.

Other admissibility credentials such as loyalty program membership and additional flight tickets for an onward journey should also be issued as verifiable-digital credentials in the digital travel wallet to share with the relevant parties ahead of the trip. The traveler should remain in full control of what credentials are included in their wallet.

APEC economies may prefer to work toward this vision of assembling admissibility credentials into one place and verifying them ahead of the trip in stages. What matters in practice is that those stages are forward-compatible with the end state, so each stage can build upon the last and maintain compatibility with other economies that are not yet ready to progress to the next stage. For example, not all admissibility documents exist in a digital form.

The interim stages should thus consider the use of:

1. Admissibility credentials that exist in digital form but are not digitally-verifiable, such as an electronic vaccination certificate with no service or application that allows for conversion into a digitally verifiable credential (or unable to verify the authenticity of the credential). Such credentials may or may not be used for advance admissibility checks but will typically require a manual verification and are at risk of being forged or tampered with.

2. Admissibility credentials that exist in digital form, are not digitally-verifiable, but can be converted into a digitally-verifiable format for issuance into the traveler's digital wallet. For example, the Airside Digital Identity App by American Airlines and Thales allows users to create a secure and encrypted digitalized version of government-issued identification which airline passengers can then store their ID on their smartphone and present it at the required checkpoints.

   To perform this conversion, the digital wallet should meet the following requirements:

   a. It must be able to validate that the original credential is authentic, being issued by the appropriate authorities and not been tampered with.

   b. It must be able to generate a verifiable credential in an agreed format aligned with adopted standards, recommended practices and technical specifications, such as ICAO's Guiding Core Principles for the Development of Digital Travel Credential (DTC) and DTC Virtual Component Data Structure and PKI Mechanisms.

   c. It must be able to be bound with the verified biometric (e.g., facial image) of the traveler.

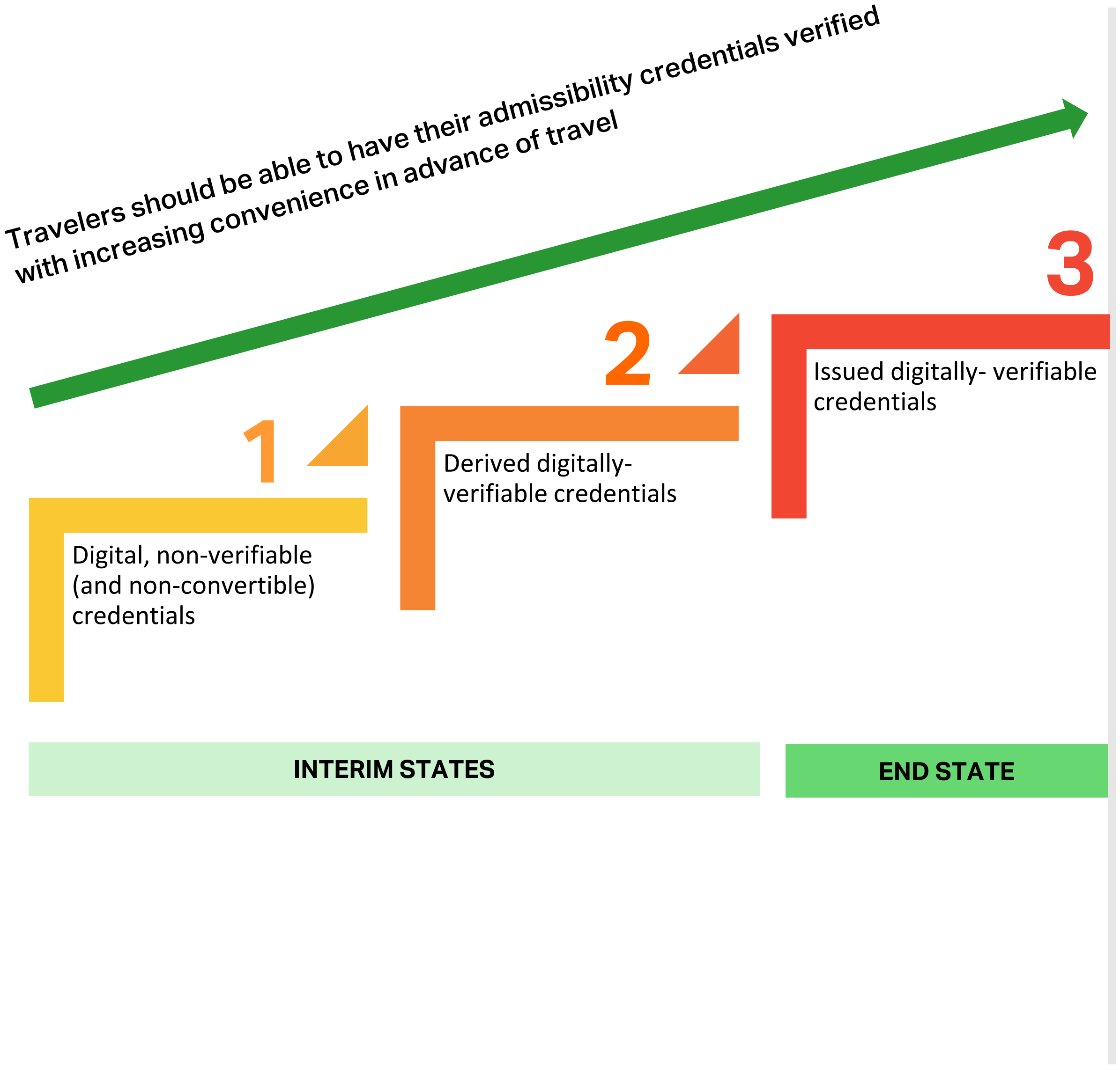
   d. All data operations should take place directly in the wallet. If any data needs to be transferred to a third-party system (e.g., to run a query against a database), such data must be anonymized and treated in a manner that no personal data can be attributed back to the credential holder.

e. The credential should contain both the data used to originally verify the source document (e.g., the digital signature of the certificate signing authority) and the verification outcome.

3. Admissibility credentials that exist in digital form and are digitally-verifiable, such as an electronic vaccination certificate with a QR code that connects to its "digital twin" stored on a legitimate clinic or health authority's website.

Figure 3 illustrates those possible interim states.

Figure 3: Possible interim states for the creation of admissibility credentials.


Travelers should be able to have their admissibility credentials verified with increasing convenience in advance of travel
1
Digital, non-verifiable (and non-convertible) credentials
2
Derived digitally-verifiable credentials
3
Issued digitally- verifiable credentials
INTERIM STATES
END STATE

2.2.2.3 Verification of admissibility

In the envisioned end state, travelers should arrive at the airport "ready to fly". This implies that the verifications of a traveler's admissibility to enter the airport areas, depart the state of origin, board the aircraft and enter the state of destination, etc. are performed prior to their reporting at the airport. The key benefits of this concept are to reduce friction (seamless travel) and congestion at the airport processors.

This end-state vision also entails that the travelers share their admissibility credentials ahead of reporting to the departure airport with various stakeholders. The verifiers that receive those credentials should temporarily store them in a secure environment, such as an Identity Management System (IMS), to reconcile those successful admissibility checks with the traveler once the latter arrives at the airport and presents themselves at each checkpoint. The IMS should only store those credentials for the duration of the next leg of the journey (e.g., the day of departure), and should store only the minimum traveler information necessary for the traveler to pass the on-airport control points (e.g., bag drop, security, exit/entry border control, and boarding). In essence, the IMS:

- Receives (and verifies) necessary information from the travelers, such as biographic data, biometric reference, and travel details.

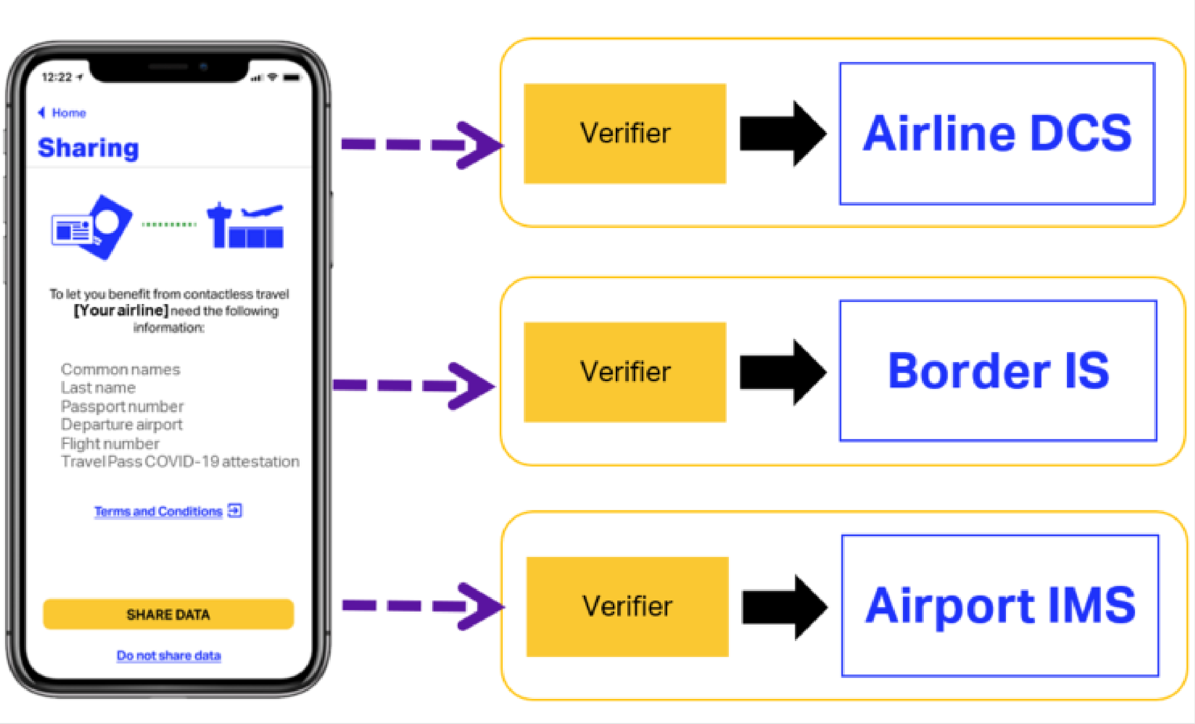
- Manages and builds a biometric gallery as required for on-airport access and other control points where identification and/or authorization is required, so that a speedy reconciliation can be performed between the traveler's biometric sample captured live and the biometric references kept in the gallery.

- Can be managed by a single stakeholder or a small collaborative effort of connected stakeholders (e.g., local stakeholders committee, airline alliance) with a trust framework and clear data roles and responsibilities established for each.

In the end state, the traveler should also be given the option to share their digital credentials (including admissibility and identity credentials) requested by the government of the destination state in advance of travel. For example, this can be done through a travel platform, as suggested by ACI and IATA in ICAO Assembly 41st session Agenda Item 13: Facilitation Programs (International Civil Aviation Organization, 2022). The state government then verifies the traveler's identity and admissibility to travel into the destination. Once approved, a notice of admissibility is issued to (or downloaded into) the traveler's digital wallet and stored as another travel credential. This mechanism differs from the current Advance Passenger Information system by anticipating the check even further, prior to departure. The airline therefore can ascertain that the traveler is entitled to enter the destination state ahead of issuing the boarding pass to the traveler's digital wallet. This mechanism removes the risk of a traveler being denied entry on arrival and saves airlines the cost of fines and repatriating the traveler.

Verifying parties should request only the minimum data for authenticity verification, and the traveler should be able to opt-out of advanced sharing of credentials for verification.

Figure 4: Selective and consented disclosure of traveler's admissibility information to the verifying parties (illustrative). DCS stands for Departure Control System and is one of the airline's systems that contains data about the traveler on a flight.



12:22

Home

Sharing

To let you benefit from contactless travel [Your airline] need the following information:

Common names
Last name
Passport number
Departure airport
Flight number
Travel Pass COVID-19 attestation

Terms and Conditions

SHARE DATA

Do not share data

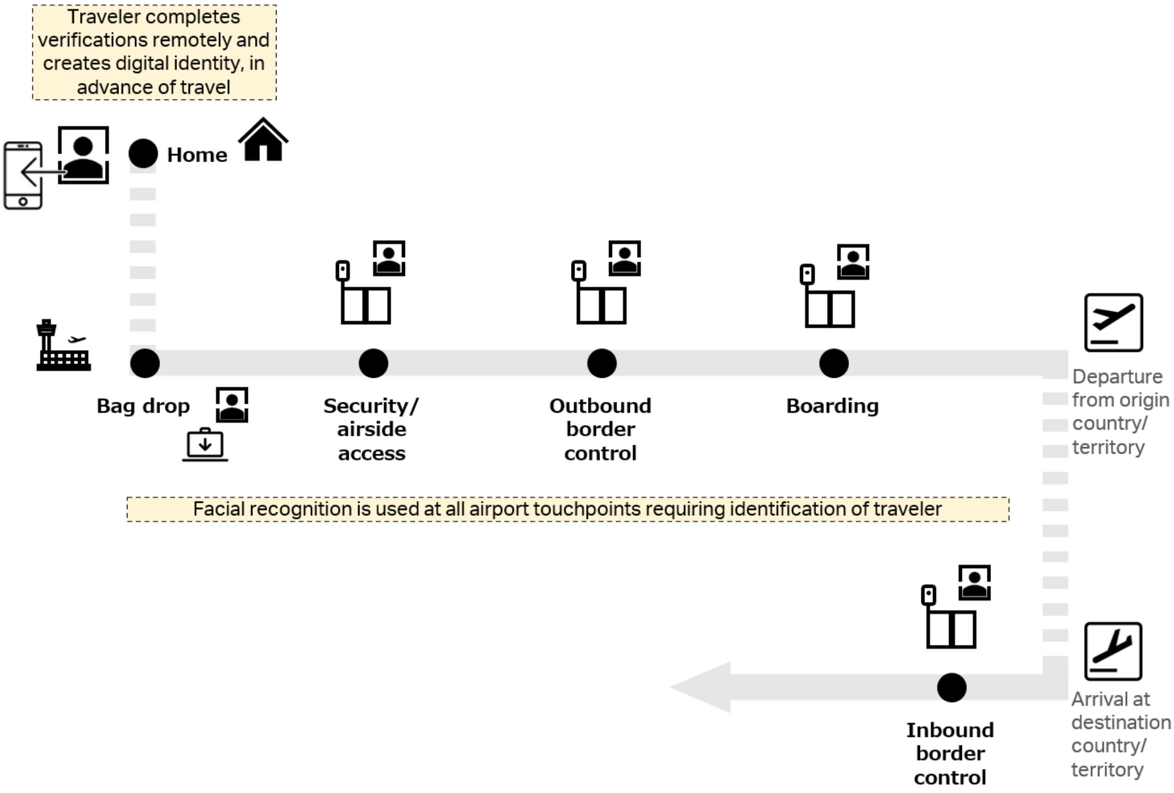
2.2.2.4 Verification of identity

The last practical step in the end-state vision is the identity verification of the traveler reporting to the airport. The traveler makes a biometric claim (i.e., that they are the source of the biometric data known about them), and this claim should be verified by reconciling their biometric sample (i.e., a live capture of their biometric by a hardware sensor at the airport) with their biometric reference contained in their digital wallet (which contains their digital identity) and shared ahead of time for temporary storage into the IMS.

If the sample and reference match, then the traveler's identity is verified, and the admissibility verification that was done prior to their reporting to the airport is probably applicable to them. At every checkpoint where the traveler's biometric is collected and verified, their biometric effectively replaces the need for the traveler to present their credentials in either digital or paper form; for all intents and purposes, their biometric (e.g., their face) is effectively and functionally equivalent to their identity document, boarding pass, entry permit, etc.

Figure 5 illustrates the typical airport touchpoints at which biometric reconciliation may be needed.

Figure 5: Contactless biometric recognition to identify travelers at the airport touchpoints


Traveler completes verifications remotely and creates digital identity, in advance of travel
Home
Bag drop
Security/ airside access
Outbound border control
Boarding
Departure from origin country/ territory
Facial recognition is used at all airport touchpoints requiring identification of traveler
Inbound border control
Arrival at destination country/ territory

3. Guidance for an implementation roadmap

The purpose of this section is to provide high-level guidance on the steps that can be taken to achieve the vision for the end state of biometric implementations in cross-border air travel. It is not meant to be a prescriptive plan, but rather, a guide that APEC economies can refer to, and make relevant changes wherever appropriate to tailor to specific needs and environment.

3.1 Establish a common vision for the end state

It is essential for the biometric implementation projects in APEC economies for cross-border air travel to begin with a vision on the end state. While this report recommended a vision for the end state of biometric implementations in cross-border air travel in Section 2, APEC economies should first achieve a mutual agreement that the proposed vision is suitable and appropriate for all economies.

In addition to an agreement across economies, this vision should also be supported by the internal stakeholders to ensure commitment towards the same direction and goal.

3.2 Dedicate a forum or task force for a coordinated implementation across APEC economies

Task forces or dedicated forums are essential within (e.g., airports, border authorities, airlines), and across the economies for APEC economies to implement biometric solutions in cross-border air travel in a harmonized manner.

The taskforce team(s) should consist of all relevant stakeholders that would be involved in the biometric ID collection and usage. Representatives from immigration and border authorities of different APEC economies are critical as they provide the expectations and requirements for security control in cross-border travel. Representatives from the airline(s) and the airport are also crucial as they provide their operational requirements and priorities.

The APEC's Transportation Working Group (TPTWG) holds regular meetings where representatives from each APEC economy and transportation sector (e.g., aviation) can discuss about specific topics, including biometrics. Such a forum can be useful to raise awareness and interest within APEC economies on biometric implementations in cross-border air travel, and for economies to showcase their progress. It can also be a platform for economies to converge on a single vision, approach and standard that is compliant with every APEC economy's regulatory and traveler processing requirements.

Subgroup(s) may also be created within a task force, so long as they coordinate with each other, as in the case of India's Digi Yatra.

During the planning phase for India's Digi Yatra initiative (which is described in further details in section 7), a Steering Committee and a Technical Working Committee were established under a single task force "Digital Cell".

The Technical Working Committee consisted of one subject matter expert from each airport and made the key decisions related to the initiative, such as the type of technology to adopt, the process to be followed, etc. These decisions were made after extensive consultations with airlines and the regulatory authorities, including the Bureau of Civil Aviation Security, Central Industrial Security Force, Intelligence Bureau, Ministry of Home Affairs, and the Unique Identity Development Authority of India.

The Steering Committee consists of the airport CEOs of the five public private partnership airports in India (Bangalore International Airport, Delhi International Airport, Hyderabad International Airport, Cochin International Airport, and Mumbai International Airport). The chairman of the Airports Authority of India (the national airport operator) was also part of the Steering Committee with the other airport operators' representatives. This committee makes the approval decisions for proposals submitted by the Technical Working Committee and is also responsible for getting formal regulatory approval requests and finances for the relevant development, operations, and maintenance.

The task force is not necessarily limited to only the stakeholders that are directly involved, as in the case of Narita International Airport Corporation (NAA)

At the planning stage of Narita Airport Authority (NAA)'s biometric implementation, the task force created included not only NAA, participating airlines (Japan Airlines and ANA), and the authority (Japan Civil Aviation Bureau), but also experts in personal data privacy matters. These experts include professors, lawyers, and the Consumer Affairs Agency. The knowledge and insights contributed by the experts allowed NAA to have a clearer picture of the legal requirements, which is essential for:

- The process and project planning,
- Obtaining the support and approval from the authority, and
- The subsequent production of a guidebook.

3.3 Consider relevant regulations

National and regional (e.g., EU) regulations need to be reviewed before making decisions. This includes (but is not limited to) the mandatory requirements for identification documents, data handling, biometric identification, as well as traveler verification processes.

A thorough assessment of the relevant regulatory requirements is essential for economies to determine and align on any required changes to regulations that may be necessary to enable the vision for the end state.

If the vision for the end state of biometric implementations in cross-border air travel is not compliant with certain regulations (e.g., digital identity) within a given economy, the economy should first consider the possibility or practicality of altering the regulations. For example, the Republic of Korea changed some of its air-travel-related regulations in 2020 so that biometric-enabled authentication of travelers could be performed at Korean airports. The regulatory changes included:

- Biometric recognition can now be used to replace manual identification checks, which were originally required in the national Aviation Security Act,
- Airports are now able to request travelers' biometric information from government agencies for biometric identification of the travelers at the airport premises (under the Aviation Security Act)
- The change in regulations also clarified the privacy level applicable to biometric information as it is collected and used for travel purposes.

Alternatively, if such regulatory changes cannot be made or agreed on, the APEC economies should consider required changes to the vision for the end state to for it to be compliant with all (participating) economies' regulatory requirements, following a reasonable "common denominator" approach. This new envisioned end state should be formally approved by the participating economies to ensure unambiguous commitment.

3.4 Set the standards, requirements, and key actions

Each APEC economy and its domestic stakeholders (e.g., border authority) possesses its own operational and regulatory requirements for processing of passengers and the use of biometric identification solutions.

These stakeholders should define the absolute minimum set of traveler information required at each processing touchpoint to comply with the need-to-know principle. As an example of a leading regulation on the matter, the European Union's General Data Protection Regulation (GDPR) requires that the data collected be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

Within each APEC economy, existing operational and regulatory needs and constraints should also be clearly communicated through a framework. This framework may include:

- People factors:
    - The roles and responsibilities of the stakeholders in relation to each other.
    - Governance mechanisms through which decisions are made, and roadblocks are escalated and removed.
- Process factors:
    - Available financial resources, time, and manpower,
    - Operational requirements for airport, airline, and border processing of travelers,
    - Issues that may impede the implementation (e.g., space constraints affecting the deployment of equipment),

  - Financial arrangements, and
  - Required changes or additions that will be needed by stakeholders in their operational processes, infrastructure, and software, i.e., the gaps to be filled before implementation,

- Technology factors:
  - Technical requirements for the solution, including data security and privacy controls, as well as other system requirements

APEC economies that intend to implement the vision for the end state should aim to act as a group, especially in working alongside APEC economies that do not intend to, or are unable to implement said vision. Such agreements can help to govern the framework with the requirements and standards for compliance. Similar agreements or policies may also be created within an economy and between the local stakeholders.

For greater interoperability across stakeholders, airports, and APEC economies, open standards should be adopted (instead of closed standards).

3.5 Conduct tests and trials within and across APEC economies

Once the plan has been defined and understood by all parties involved, biometric testing should be conducted before production roll-out to identify and correct process and technology issues. The biometric solution should be tested to ensure that it is able to:

- Work under all conditions encountered on and off-airports, including in different locations, lighting conditions, crowds, etc.
- Cope with different appearances of the passenger, e.g., with glasses, beard, hair color, etc.
- Perform processes, including the biometric capture and matching while a passenger is approaching the touchpoint within a desired duration, for contactless biometric recognition.
- Achieve the expected or required accuracy rates.

- Effectively detect biometric presentation attacks, to a desired or required confidence level.

Trials are essential for a collaborative cross-border passenger processing biometric implementation by two different APEC economies. Implementations that only involve a single economy, airport, or airline are no longer new to the aviation industry. However, cross-border collaboration to enable a fully biometric-enabled traveler journey from the origin airport (departure) to destination airport (arrival) do not have multiple success cases as of time of report writing to establish robust expected outcomes, results, or issues. For example, the progress of the pilot of "Known Traveler Digital Identity" service that enables paperless border clearance between Canada and The Netherlands (i.e., passengers can clear departure touchpoints, as well as arrival immigration with just facial recognition) has been affected by the pandemic, with no news on restart as of the date of report writing. Through the trials, stakeholders (depending on their scope of business operations) should ascertain:

- If the travelers and verifiers can use and operate the solution as intended,
- If the process can achieve the intended outcome, i.e., a seamless traveler journey at the airport through advanced verifications and on-airport biometric identification
- If there are any technical issues with the solution (e.g., unable to achieve the desired or required accuracy rate)
    - It is essential to ensure that the recognition system produces a higher accuracy rate than if manual checks by a staff was conducted, i.e., less false positives and false negatives.

Any issues that have been identified during the tests and trials (e.g., unacceptable level of accuracy or false positives when used by a certain group of users or under certain conditions), or gaps between the operational process and the intended process (e.g., the ease of usage of the system by passengers when unguided) should be fixed before the actual roll-out.

3.6 Adoption

Production roll-out should follow a similar staged approach as trials, i.e., through the gradual introduction of interim states that increase the maturity of the implementation over time. For example, the biometric implementation can first be done locally, followed by bilateral collaboration between two APEC economies, within a small group of APEC economies, and eventually all APEC economies (if applicable).

4. Key success factors

4.1 Government's collaboration and buy-in

Government support was raised by multiple stakeholders as a key success factor in biometric implementations in cross-border air travel. This could be in the form of:

- Domestic policies,
- Endorsed or published guidance,
- Communication of goals for biometric ID implementations to the relevant stakeholders (airlines, airports, border control); and,
- Financial support.

Stakeholders have also identified the government's support as a driver for airline participation and the public's acceptance of the concept, which are crucial to the adoption rate, degree of success, and extent of improvement in efficiencies.

The buy-in from immigration or border control of an economy, combined with that of the private sector, is necessary so that both commercially managed touchpoints (e.g., check-in, boarding) and regulatory touchpoints (e.g., border control, customs) can utilize biometric identification solutions. This would then enable a fully biometric-enabled journey for travelers.

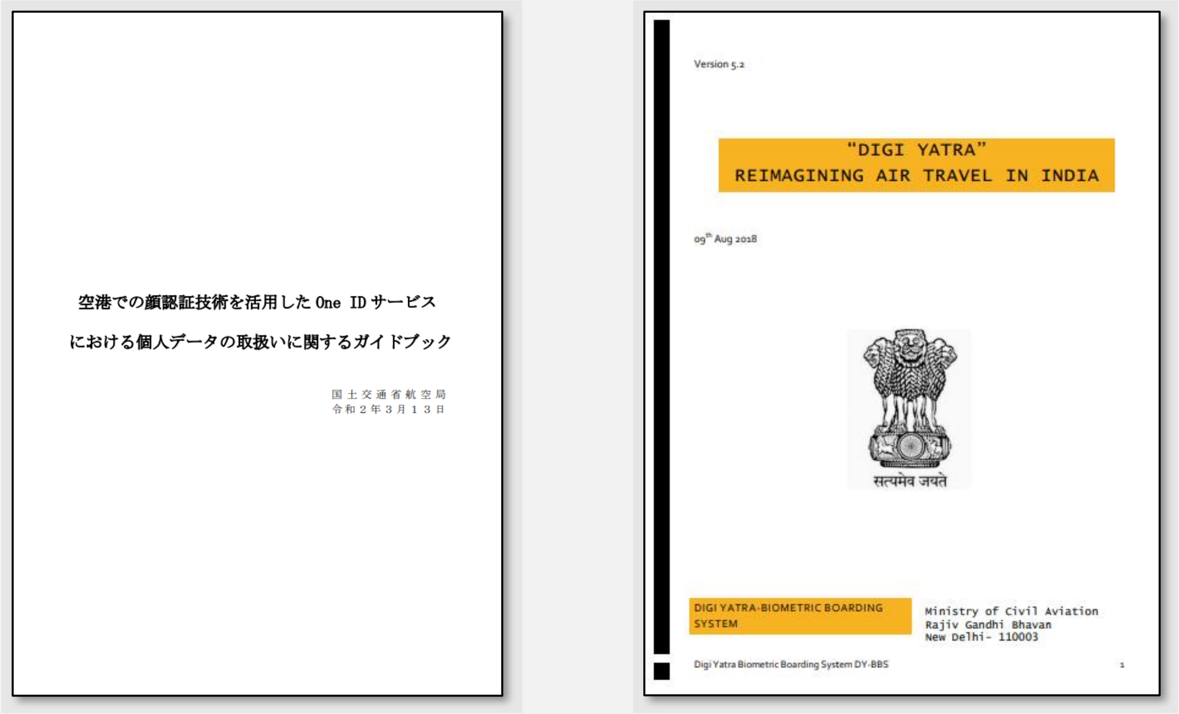
Example

For instance, the Japan Civil Aviation Bureau (JCAB) released and endorsed a guidebook: Guidebook on personal data management in One ID[5] service at the Airports (MLIT Japan Civil Aviation Bureau, 2020) in 2020. Narita International Airport Corporation and other experts heavily supported the guidebook's production. This guidebook can also be used by other airports in Japan subsequently as reference before they begin any form of biometric implementations.

Similarly, Bangalore International Airport Limited approached India's Ministry of Civil Aviation to propose the biometric ID concept, and after discussions, a national policy: the

[5] One ID is an initiative by International Air Transport Association that introduces an opportunity for the traveler to further streamline their journey with a document-free process based on identity management and biometric recognition.

Digi Yatra Policy (Ministry of Civil Aviation, India, 2018) was released by India's Ministry of Civil Aviation.



空港での顔認証技術を活用したOne IDサービス

における個人データの取扱いに関するガイドブック

国土交通省航空局
令和２年３月１３日

Version 5.2

"DIGI YATRA"
REIMAGINING AIR TRAVEL IN INDIA

09th Aug 2018

सत्यमेव जयते

DIGI YATRA-BIOMETRIC BOARDING SYSTEM

Ministry of Civil Aviation
Rajiv Gandhi Bhavan
New Delhi- 110003

Digi Yatra Biometric Boarding System DY-BBS 1

Figure 6: Japan's Guidebook on personal data management in One ID service at the Airports (left) (MLIT Japan Civil Aviation Bureau, 2020) and India's Digi Yatra Policy (right) (Ministry of Civil Aviation, India, 2018)

4.2 Transparent communication

Consistent and transparent communication is the most common key success factor identified by stakeholders. It includes communication between the private sector, the relevant authorities, the travelers, the solution provider(s), and within the organizations. The expected actions of each stakeholder during planning and implementation need to be clearly defined.

Frequent and transparent communication also increases every stakeholder's participation, introduces different perspectives, and value-adds from different aspects. Stakeholders should align on the needs and requirements of each stakeholder as well as potential challenges and respective solutions.

Within the organization:

Individuals/ teams responsible for separate aspects (e.g., technical team, legal team) should have a broad view of what the other individuals/ teams are doing.

With authorities:

Authorities should be kept in the loop during the planning and implementation, and more importantly, be informed of how the process works and aligns with the national and regional regulations.

The authorities should also set out clear requirements to the implementing party on the process (e.g., requirements of border control) and data management (e.g., data privacy protection). They should also ensure alignment on:

- Interpretation of regulations (e.g., relevant equivalents of privacy regulations such as GDPR).
- Understanding of cybersecurity matters, data access, storage duration and purpose, and security levels that will be in place.

With travelers:

Travelers should be well notified on the type of data collected, shared, and used for processing, the parties that will have access to those data, the storage period, the purpose of using the data, and their ability to choose to use and share biometric data or not.

With solution providers:

The vendors need to be provided with the specifications, especially on the accuracy rate expected. Based on interview findings, some stakeholders approached the vendors without expected accuracy rates (and the rationale behind it) and resulted additional internal discussions required during the implementation period. This further resulted in in a longer implementation duration.

Example

For instance, without advertisements, Fraport managed to increase the biometric adoption rate by 10-30% every month at Frankfurt Airport, driven by a strong focus on transparent communication to the travelers. The airport clearly informed travelers that they are the data owner, and that the biometric data is the self-sovereign identity of the traveler. With this understanding, travelers were motivated by the convenience of biometric processing and did not require promotions initiated by the airport to join the program.

Fraport also established multiple teams with specific purposes (e.g., steering committee, technical team, legal team), with each team having its own 'roadmap' defining the actions that need to be taken. A strong understanding of the implementation was expected across all teams – for example, the legal team had to be familiar with the process and traveler flow to inform the technical team of the associated requirements.

In another example, the Airport Authority of Hong Kong (AAHK) also held regular meetings with not only airlines, but also the Civil Aviation Department (CAD) to provide implementation progress updates. Through these meetings, the CAD ensures that what the airport is doing complies with the safety and security levels required.

4.3 Understanding the regulations

Regulations on data management, e.g., data privacy and protection, vary across economies and regions. Moreover, a single set of regulations can be interpreted differently across different economies or even within an economy. As such, it is essential to establish a common understanding across all stakeholders on the regulations within the scope of implementation. This includes requirements on the handling travelers and data, as well as the geographical applicability.

Example

For instance, Narita International Airport Corporation (NAA)'s task force for their biometric implementation included airlines, the authority (Japan Civil Aviation Bureau, JCAB), as well as experts in personal data privacy and protection. The experts (e.g., professors and lawyers) were involved in the planning, even before NAA approached JCAB.

The efforts made in establishing a strong understanding of the regulatory requirements (with the help of the experts) increased NAA's and JCAB's confidence that the implementation would be compliant with regulatory requirements. It was also a convincing factor for JCAB's support in the project and sped up the implementation process. The findings and knowledge based on discussions with the experts also contributed to the development of the guidebook published and endorsed by JCAB.

In another example, Fraport conducted multiple discussions with various governments to establish a mutual understanding and agreement on the interpretation of the GDPR. It was noted that different governments – across or even within countries (e.g., different state governments) interpret the GDPR differently, preventing the use of a single solution or process for all economies.

It also took Fraport about a year of discussions with legal teams of different stakeholders, such as airlines, technical providers, authorities, and airports to understand and establish a clear idea of an implementation that is fully compliant with the applicable regulations and requirements. While this is a challenging and time-consuming process, it was crucial to ensure complete alignment of the process and data management with the legal requirements of the economy and region.

4.4 Keeping a clear end goal/ outcome in mind but being open and flexible in the process

Stakeholders should keep an open mind and be prepared to implement changes to established processes and solutions for greater efficiency in the implementation process. This is especially so for infrastructural changes which may be required to accommodate biometric systems for optimal processing. Stakeholders approaching vendors should have an end goal or outcome in mind (e.g., how they wish their border control would look in 5 to 10 years), with specifications such as accuracy rate determined beforehand, yet maintaining flexibility on the process to reach that outcome.

Example

For instance, solution providers mentioned that infrastructural changes may be required for the appropriate lighting conditions for a facial recognition system and a certain accuracy or detection rate. When stakeholders implementing biometric solutions at airport showed inertia or reluctance to make such changes, further discussions need to be conducted that increases the duration and reduces the efficiency of the implementation process.

5. Key benefits of biometric ID use in aviation and its harmonization

5.1 Improve traveler satisfaction

Biometric-enabled traveler processing can improve the airport experience for travelers by eliminating repetitive processes and possibly combining or reducing the number of touchpoints. This results in shorter queues, or no queueing at all in the end-state vision, and reduced waiting times.

For example, before the implementation of the biometric identification Digi Yatra initiative, manual checks by staff were conducted on travelers' identity and travel documents (including vaccination status) at the entry gate of Indian airports.

- The staff first checks the travel document, the date, and the time of the flight (to ensure that it is within the four-hour window) before allowing the traveler to proceed.
- A second check is conducted to validate that the name of the traveler on the identity card is the same as the name on the travel document.
- A third check is then conducted to match the face of the actual person to the photograph shown on the identity card.

This entire process was cumbersome and took approximately 15 to 20 seconds or longer (e.g., if the travel document is in PDF format that is too small to be easily read). Based on test results, biometrics recognition simplifies the process and takes 7-9 seconds at maximum.

Similarly, at Indian airports, the bag drop touchpoint generally requires around 90 seconds for an average for a traveler to check in a bag. Based on test results, this duration would be halved with the biometric solution.

5.2 Increased efficiencies and reduced manpower

Processing travelers using biometric identification methods reduces processing time compared to manual checks. This in turn improves capacity for processing more travelers, reduce the required manpower for manual checks, and enable alternative staff allocation (e.g., risk-based screening).

For instance, with biometric boarding at Heathrow Airport T5, British Airways reduced domestic flight boarding time by 33% and the number of gate staff from three to two at each gate.

India's Digi Yatra biometric and e-gates solution prevents the mixing of domestic and international travelers at their designated areas. Without the biometric solution, travelers may enter the non-designated areas without being aware of it until they pass through the security check process. This then creates a problem for airport as the traveler needs to be directed out of the wrong area.

5.3 Enhanced security and accuracy

Biometrics improves border, aviation, and airport infrastructure security by reducing the possibility of individuals crossing borders under a false identity, and thus help combat human trafficking and other cross-border criminal activities. It also enables risk-based assessment and differentiated handling at border and security.

A biometric automated access control system verifies the identity of the person requesting access, while other systems only verify the identity document (which may be lost, forged, or stolen) and the personal identification number (which may be divulged by the user or compromised).

6. The common types of biometric ID

ICAO considered several biometric technologies and focused intensively on the generic types of biometric technologies including face image, iris, fingerprint, hand geometry, and voice in its 2001 evaluation. While retinal features and other biometric technologies were also considered, they were rejected as impractical means of identity confirmation, given the requirements for machine-assisted identity confirmation when presenting an MRTD (International Civil Aviation Organization, 2007).

While multiple types of biometric identification methods are available to be used to process travelers at airport touchpoints. However, facial recognition is used in our recommended vision for the end state of biometric implementations in cross-border air travel due to its prevalence worldwide, its suitability for international standards (e.g., ICAO), and its contactless nature.

6.1 Fingerprint

Fingerprint is the oldest and the most used biometric trait in identification problems due to its wide user acceptability, accuracy, security, and relatively inexpensive cost (Belhadj, 2017).

Fingerprint recognition achieves a higher level of security due to its high uniqueness and maturity. It is also increasingly cost-effective over time with increased adoption in the industry and by users. However, although fingerprints do not change significantly over time, they get worn out (e.g., older people with a history of manual work may struggle with worn prints), affecting the quality of the registered fingerprint images (NEC, 2022).

The error rates and quality of the fingerprint image are affected by factors such as (Alonso-Fernandez, et al., 2009):

- Skin conditions (e.g., worn out prints of older individuals, dryness, wetness, dirtiness, temporary or permanent cuts and bruises on the fingerprint),
- Sensor conditions (e.g., dirtiness, size), and
- User cooperation.

Such conditions and situations may or may not be avoidable and affects the quality of the recognition results of the biometric system.

6.2 Iris Recognition

Iris recognition involves capturing photos or video images of a person's eyes and mapping the unique iris pattern to verify identity. This makes it non-invasive, and no physical contact is needed in the process. Any attempt to change the iris patterns (e.g., with surgery) comes at a high risk, unlike the fingerprint trait which is relatively easier to tamper with (Alaa S., Qahwaji, Ipson, & Al-Fahdawi, 2017). It is thus considered the most secure biometric trait against fraudulent methods and spoofing attacks by an imposter. In addition, no physical or digital trace of a person's iris is left, limiting the dangers and risks of spoofing (IDEMIA, 2021).

The pattern of an iris is complex, unique, resistant to aging, and practically impossible to replicate, allowing its data to act as an identifier unique to each individual.

An iris scan provides almost 250 feature points for matching, while a fingerprint provides 100 feature points (Singapore Immigration & Checkpoints Authority, 2020). Iris recognition is thus more robust and reliable for use for identification (than other biometrics like fingerprint). In addition, specialized equipment is required to conduct the iris scan, making it less susceptible to misuse.

The iris data does not have gender and ethnic bias since nothing except the detail of the iris pattern is considered when verifying a person's identity. Unlike fingerprint verification which is affected by factors like deterioration of fingerprints due to aging, scarring, or dryness, iris recognition is not subjected to such circumstances.

6.3 Facial Recognition

Facial recognition has become the dominant solution in biometric identification. Biometric identity documents issued by more than 120 economies contain a JPEG image of the bearer's face.

When compared to fingerprints and irises, facial recognition has a higher level of collectability and acceptability but a lower level of distinctiveness (Jain, Ross, & Prabhakar, 2004). Nevertheless, biometric facial recognition still reaps a higher rate of accuracy in identification than when done manually. For example, the GaussianFace algorithm developed in 2014 by researchers at The Chinese University of Hong Kong achieved facial identification scores of 98.52%, higher than the score of 97.53% achieved by humans (Pandey, Yadav, & Pandey, 2020).

In 2002, ICAO endorsed face recognition as the globally interoperable biometric for machine-assisted identity confirmation with MRTDs in the Berlin Resolution (International Civil Aviation Organization, 2007). The advantages of facial recognition include (ICAO, 2015):

- Facial photographs do not disclose information that the person does not routinely disclose to the public.
- The photograph (facial image) is already socially and culturally accepted internationally.
- The facial image is collected and verified routinely as part of the eMRTD application form process to produce an eMRTD to Doc 9303 specifications.
- The public is already aware of the capture of a facial image and its use for identity verification purposes.
- The capture of a facial image is non-intrusive. To be enrolled, the end user does not have to touch or interact with a physical device for a substantial timeframe.
- Facial image capture does not require introducing new and costly enrollment procedures.
- Capture of a facial image can be deployed relatively immediately, and the opportunity to capture facial images retrospectively is also available.
- Many states have a legacy database of facial images captured as part of the digitized production of travel document photographs, which can be verified against new images for identity comparison purposes.
- In appropriate circumstances, as decided by the issuing State, a facial image can be captured from an endorsed photograph, not requiring the person to be physically present.
- For watch lists, a facial image is generally the only biometric available for comparison.

- Human verification of the biometric against the photograph/person is a relatively simple and familiar process for border control authorities.

6.4 Palmprint

Palmprint recognition uses unique discriminative features of palmprints to identify a person (Zhang, Yue, & Zuo, 2011). Like fingerprints, the surface of the palm contains ridges and valleys.

Despite the similarity, palmprints has some advantages over fingerprints, such as having additional features (e.g., wrinkles and principal lines) that can be easily extracted from slightly lower-resolution images. As it can provide more information than fingerprints, palmprints can make an even more accurate biometric system (Dhiman, Gupta, & Sharma, 2021). When using a high-resolution palmprint scanner, multiple hand features, including geometry, ridge and valley features, principal lines, and wrinkles, can be combined to build a highly accurate biometric system (Brown, 2018).

In addition, it is more difficult for palmprints to be spoofed than for facial images, which are a public feature, or fingerprints, which leave traces on many smooth surfaces (Ungureanu, Salahuddin, & Corcoran, 2020).

However, despite fingerprints and palmprints both having uniqueness and permanence, which make them a trusted form of identification, the development of palm recognition has been comparatively slower.

6.5 Hand (and finger) Geometry

Finger geometry considers the shape and measurements of the finger and does not provide a unique biometric the way fingerprints or iris do (Types of Biometrics: Finger Geometry – Key Considerations, 2022). However, the technology can be used for identity verification for large volumes of users where identity assurance or security requirements are lower. Hand geometry biometric systems incorporate the salient features of finger geometry, the surfaces of the hand itself, and its side profile. The length, width, thickness, and surface area of the individual's hand are measured and recorded (Types of Biometrics – Hand Geometry, 2022). Advantages of this identification method include (Duta, 2009):

- Hand shape can be captured in a relatively user-convenient, non-intrusive manner by using inexpensive sensors,
- Extracting the hand shape information requires only low-resolution images, and the user templates can be efficiently stored, and
- This biometric modality is more acceptable to the public as it lacks criminal connotation.

While hand geometry recognition systems are fast and simple to implement, they work better with a small dataset. When a larger number of people is analyzed, the possibility of having two or more individuals with the same hand geometry data increases. Such systems are also deficient in identifying and differencing the left and the right hand, and distinguishing between a pair of twins (Raimugia, Patel, Pawar, & Deulkar, 2014).

The downside of hand geometry recognition is its relatively lower uniqueness (compared to other technologies like iris and fingerprint), and its effectiveness and performance can also be affected by other factors such as swelling or injury of the hand which changes its shape, and hand geometry could also evolve with an individual's weight and age. Hand geometry is also not sufficiently distinctive enough to allow a search against a large database and is generally limited to a direct comparison against a single data (e.g., biometric template), making it less suitable for identification but more for verification (Al-Ani & Rajab, 2013).

6.6 Voice Recognition

Voice is a combination of physical and behavioral biometric characteristics. The physical features of an a person's voice are based on the shape and size of the vocal tracts, mouth, nasal cavities, and lips used in making sounds. Voice recognition usually measures the formants or sound characteristics that are unique to each person's vocal tract.

Voice recognition allows for incremental authentication protocols, i.e., a higher degree of confidence can be achieved through a more complex and longer voice. For example, more voice data can be captured when a higher degree of recognition confidence is needed. However, voice recognition comes with several disadvantages when compared to the other forms of biometric identification. With the improvement of text-to-speech technology and trainable speech synthesis, automatic systems can imitate a given person speaking

(Majekodunmi & Idachaba, 2011). The performance of a voice recognition system is also susceptible to external factors like background and channel noise, microphone capabilities, etc.

6.7 Gait

Gait recognition is one of the few biometric traits that can be used to recognize people at a distance as it analyzes the way an individual walks. This makes it more suitable for surveillance (Ross & Jain, 2007).

While this behavioral identification method is non-invasive and can be easily acquired from a distance, it has lower accuracy and reliability (Sabhanayagam, Venkatesan, & Senthamaraikannan, 2018). In addition, several factors impact an accurate capture and assessment of gait information, including variations in views, clothing, changes in age, etc. Gait data is also more difficult to collect than other biometric data like facial images or fingerprints as it requires a larger storage and the associated cost. Gait recognition systems with high accuracy may also cause more privacy problems than face recognition systems, as gait information can be captured further away than facial images can (Shen, Yu, Wang, & Hua, 2022).

7. Case studies

7.1 India's Digi Yatra

7.1.1 Background

Building on the previous initiative of authenticating travelers against the government Aadhaar[6] database at the start of every trip, which had numerous privacy and confidentiality issues, the Ministry of Civil Aviation, together with other relevant stakeholders, has developed the new "Digi Yatra" platform. Digi Yatra is a new form of digital ID unique to each traveler (linked to their biometrics). It aims to enable a completely paperless boarding process for travelers. This initiative is expected to begin phased implementation across Indian airports by March 2023.

7.1.2 How it works

The first step for a traveler is to install the Digi Yatra Central Ecosystem (DYCE) enrolment application. The one-time enrolment process starts with the traveler entering the AADHAAR or driving license number. The face biometric is extracted from AADHAAR database (based on the identity number provided by the traveler), and the passenger is prompted to take a facial image ("selfie") to validate against the extracted facial biometric. Upon a successful match, the traveler's digital identity credential is created, encrypted, and stored in the secure wallet in the traveler's own smartphone (DYCE application). Similarly, health data is obtained from the CoWIN[7] portal, and the health credentials are created, encrypted, and stored in a secure wallet. Whenever travel is planned, the traveler uploads or scans the boarding pass or electronic ticket, and the travel credentials are created, encrypted, and stored in the secure wallet.

Alternatively, travelers may use the registration kiosks outside the airport for enrollment (for exceptions such as when a match during enrolment using the mobile application fails).

[6] Aadhaar is a 12-digit unique identity number assigned to the residents of India. The number is linked to the resident's basic demographic and biometric information, such as a photograph, ten fingerprints, and two iris scans.

[7] CoWIN is India's Covid Vaccine Intelligence Network; a tech-based platform facilitating the planning, implementation, monitoring, and evaluation of Covid-19 vaccination in India.

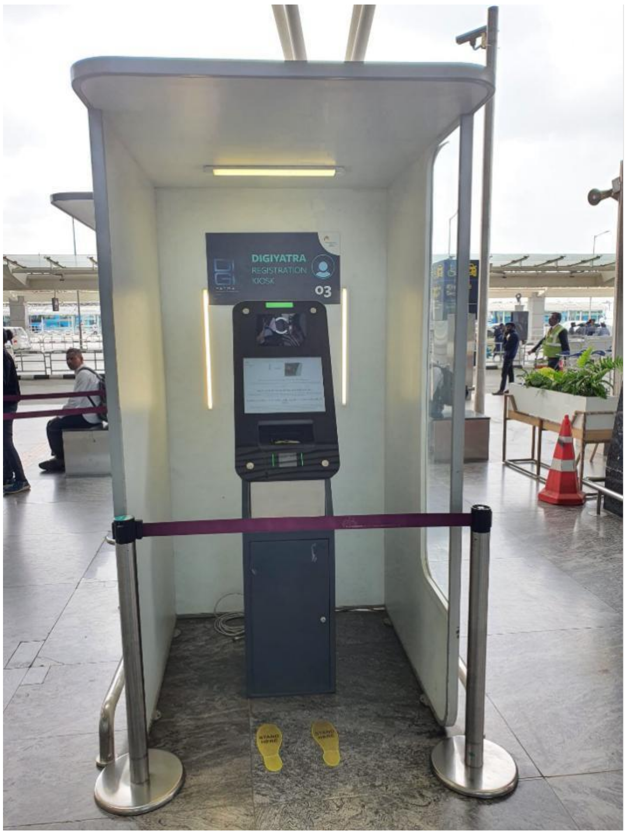


Figure 7: Digi Yatra registration kiosk outside Kempegowda International Airport Bengaluru

After enrollment, once the traveler arrives at the airport, they can scan the boarding pass or electronic ticket at the e-gates (for airport terminal entry) for his/her facial image to be captured. This 'face of the day' is validated and verified against the face biometric from the identity credential created during enrollment. The admissibility verifiable credentials are validated with travel information in the airline Departure Control System (DCS). Upon successful completion of the checks, the e-gates open to allow the traveler to enter the airport. The traveler can then be validated using the same face biometric data at all the remaining touchpoints at the airport check-in kiosk, self-service/assisted baggage drop, pre-embarkation security check entry, boarding gates, etc.

7.1.3 Ownership and usage of data

In the previous initiative, privacy, and confidentiality of the traveler's personal information (Aadhaar ID) were not well-protected (Aadhaar numbers were printed on some travelers' boarding passes, violating the Aadhaar Act 2016). Since then, the government has learned its lesson and ensured a stringent data protection mechanism before implementing this digital scheme. A Committee of Experts was set up by the government to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill, and draft such a bill. In late 2017, the committee published a white paper on data protection: White Paper of the Committee of Experts on a Data Protection Framework for India (Committee of Experts, 2017).

The Digi Yatra Central Ecosystem (DYCE) ensures that there would not be any central storage of travelers' personally-identifiable information (PII) data. The PII data will be encrypted and stored in the traveler's smartphone in a secure wallet in the DYCE application. Travelers would be able to store their digitally-verifiable credentials like those for identity, health, travel (e.g., entry permits) in their own secure wallet in the smartphone/DYCE application.

Through the DYCE enrolment application, travelers would be able to consent to share their verifiable credentials (identity, health, travel, etc.) to the relevant verifiers such as airports, or regulatory agencies like Bureau of Civil Aviation Security (BCAS), Central Industrial Security Force (CISF), or immigration whenever they travel.

7.2 Aruba Happy Flow

7.2.1 Background

Happy Flow was developed in a collaborative effort of the Aruba Government, Aruba Queen Beatrix International Airport (AUA), the Dutch Government, KLM, the Schiphol Group, and Vision-Box. A two-year pilot project was introduced at AUA in 2015 and completed in 2017.

Happy Flow uses biometric authentication, specifically the traveler's facial image as the main identification token instead of the identity document and boarding pass to verify the traveler's identity throughout the entire traveler journey at the airport. The traveler is only required to show their identity document once, at check-in, when enrolling their biometric data.

The project has been expanded to both arrivals and departures with new Automated Border Control e-Gates since 2018, with a dedicated Automated Border Control area inaugurated for USA Departures.

7.2.2 How it works

Travel documents are only required once, at check-in for enrolment. The traveler's identity is checked, and a virtual identity is created. After check-in, the traveler goes through baggage drop-off, security access, border control and boards the aircraft by facial recognition and without the need to show any travel document(s). At traveler touchpoints, including self-service bag drop, automated security access, border control e-gates, and self-boarding gates, each traveler's face is identified and matched to a fully secured database, and only authorized travelers are allowed to move on.

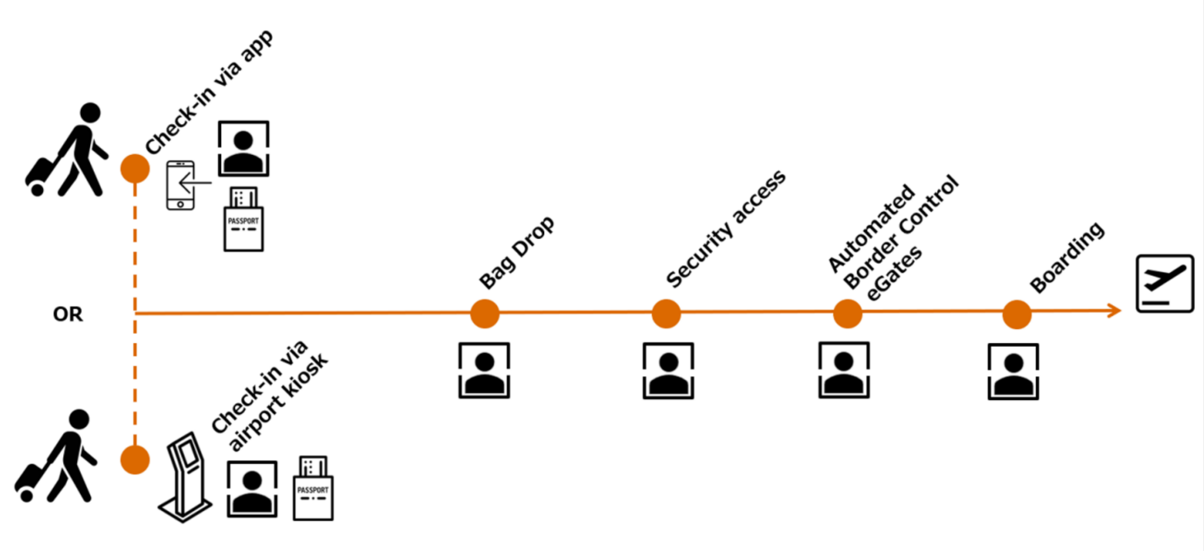


Figure 8: Overview of Aruba Happy Flow traveler journey

7.2.3 Ownership and usage of data

The whole Happy Flow project rests on a local trust framework i.e., a public/private partnership whereby the stakeholders, including the airport, airline, and border security (government) collectively own the system, and each stakeholder could access information on an authorized-to-know and a need-to-know basis.

The platform adheres to the internationally recognized "privacy by design" standard, and the architecture and design reflect GDPR privacy compliance standards, ensuring accountability and strong governance are built into the system. The Passenger Data Envelope that is created using the traveler's biographic information and captured facial image is only stored for 24 hours.

8. Appendix: Global standards and guidance

8.1 Privacy by design

Privacy by design is a concept that advocates the integration of privacy into data systems and technologies at every stage of the design process to reflect a "design thinking" perspective, i.e., data protection through technology design. The seven foundational principles of Privacy by Design (Cavoukian, 2011) are:

I. Proactive, not reactive; preventive, not remedial: Privacy by Design framework prevents privacy-invasive events before they happen instead of waiting for privacy risks to materialize or offering remedies for resolving privacy infractions once they have occurred.

II. Privacy as the default setting: Ensure that personal data are, by default, automatically protected in any given IT system or business practice without any action required by individuals to protect their data.

III. Privacy embedded into design: Privacy is an essential component embedded into the design and architecture of the IT system and business practice and is integral to the system without diminishing the system's functionality.

IV. Full functionality – positive-sum, not zero-sum: Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum approach, where unnecessary trade-offs are made, e.g., privacy vs. security - it demonstrates the possibility to have both.

V. End-to-end security – full lifecycle protection: Strong security measures are essential to privacy, from start to finish, to ensure all data are securely retained and then securely destroyed at the end of the process in a timely fashion. It ensures cradle-to-grave, secure lifecycle management of information end-to-end.

VI. Visibility and transparency – keep it open: Seek to assure all stakeholders that:

- Regardless of the business practice or technology involved, it is operating according to the stated promises and objectives, subject to independent verification, and

- Its component parts and operations remain visible and transparent to users and providers.

VII. Respect for user privacy – keep it user-centric: Keep the interests of the individual as the largest priority by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options, keeping it user-centric.

8.2 ICAO Digital Travel Credentials

In 2020, ICAO published a set of guidance for the development of Digital Travel Credential (DTC) (ICAO, 2020), and listed the 3 types of DTC implementations:

- Type 1: eMRTD bound DTC consists of a DTC-VC[8] only, with the eMRTD[9] as a physical authenticator. The DTC-VC is derived from an existing identity document by extracting the data from the chip in the document. In this type, the physical authenticator will be the identity document booklet.

- Type 2: eMRTD- PC bound DTC consists of a DTC-VC and a DTC-PC[10] in addition to the eMRTD, with the DTC-VC (signed by the issuing authority's public key infrastructure) derived from an existing travel document with the option to store the DTC-VC in a remote system (e.g., database, web service) or store it elsewhere (e.g., smart device). The issuing authority will create the DTC-PC on a physical device (such as a smartphone) that the issuing authority or the holder may supply. This is digitally signed by the issuing authorities Public Key Infrastructure (PKI). Both the device, i.e., the DTC-PC and the identity document can be physical authenticators.

- Type 3: PC bound DTC consists of a DTC-VC and a DTC-PC but no eMRTD. The issuing authority will create the physical authenticator of the DTC on a physical device (e.g., a mobile phone) which will serve as the DTC-PC. There is no connected physical identity document in this type.

Both type 1 and type 2 DTCs are suitable for biometric solutions for seamless aviation travel.

[8] The VC, or virtual component of a DTC containing the digital representation of the holder's identity.

[9] An MRTD that has a contactless integrated circuit embedded in it, the capability of being used for biometric identification of the holder and conforming with the specifications contained in Doc 9303.

[10] The DTC-PC refers to the physical component of a DTC that is cryptographically linked to the virtual component.

For Publication on the ICAO Website

Guiding Core Principles
for the Development of
Digital Travel Credential (DTC)

DISCLAIMER: All reasonable precautions have been taken by ICAO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied; nor does it necessarily represent the decisions or policies of ICAO. The responsibility for the interpretation and use of the material contained or referred to in this publication lies with the reader and in no event shall ICAO be liable for damages arising from reliance upon or use of the same. This publication shall not be considered as a substitute for the government policies or decisions relating to information contained in it. This publication contains the collective views of an international group of experts, believed to be reliable and accurately reproduced at the time of printing. Nevertheless, ICAO does not assume any legal liability or responsibility for the accuracy or completeness of the views expressed by the international group of experts.

Version 4.4

October 2020

File: Guiding Principles for the Development of Digital Travel Credential Specifications (DTC).doc
Author: ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP), Subgroup of the New Technologies Working Group (NTWG)

Figure 9: ICAO Guiding Core Principles for the Development of Digital Travel Credentials (DTC) (ICAO, 2020)

8.3 World Wide Web Consortium (W3C) standards on verifiable credentials

The W3C standard defines a verifiable data registry as "*A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials*". Examples of verifiable data registries include "*trusted databases, decentralized databases, government ID databases, and distributed ledgers*".

To enable the verifier to trust the issuer to issue the credential that it received, a credential is expected to either (World Wide Web Consortium, 2022):

- Include proof establishing that the issuer generated the credential, or have been transmitted in a way clearly establishing that the issuer generated the verifiable credential, which was not tampered with in transit or storage,

- All entities trust the verifiable data registry to be tamper-evident and to be a correct record of which data is controlled by which entities,

- The holder and verifier trust the issuer to issue true credentials about the subject and to revoke them quickly when appropriate, and
- The holder trusts the repository to store credentials securely, not release them to anyone other than the holder, and not corrupt or lose them while they are in its care.

8.4 IATA Recommended Practice

IATA will be publishing a set of Recommended Practices (expected to be published by the end of 2022) that covers:

- The handling of the biometric data once received (including the verification requirements), though all appropriate privacy and data protection regulations must be adhered to in implementations
- The Border entry, exit, and transit touchpoints
- Other biometric modalities, including but not limited to fingerprint, iris, and palm vein.
- Trust frameworks for W3C Verifiable Credentials and Decentralized Identifiers (e.g., the expectations of a credential and its creation for the verifier to trust the issued credential).

8.5 General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) was implemented in 2016, mandating EU members to incorporate it into their national laws by May 2018. The GDPR limits the ability for cross-border transfers of personal data and generally requires that the receiving country has adequate data protections in place. In 2018, the EU also implemented additional rules to protect the privacy rights of its residents when dealing with public EU institutions.

The Regulation (European Union, 2016) protects E.U. citizens and long-term residents from having their information shared with third parties without their consent, and established that data processing is only lawful if:

I. The data subject has given consent to the processing of his or her personal data for one or more specific purposes,

II. Processing is necessary for the performance of a contract to which the data subject is party,

III. Processing is necessary prior to entering into a contract, at the request of the data subject,

IV. Processing is necessary for compliance with a legal obligation to which the controller is subject,

V. Processing is necessary to protect the vital interests of the data subject or of another natural person,

VI. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or

VII. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For biometric-enabled airport processing, key requirements include:

- The required explicit consent from the traveler before data collection,
- The right for the traveler to withdraw his/her consent at any time,
- If a data breach is discovered, processors must inform the authorities within 72 hours of discovery, and
- Data usage should be limited to what is necessary, collected for "specified, explicit and legitimate purposes", managed carefully and sensibly.

8.6 ICAO-recommended compliance of biometric applications to ISO standards

Application	Standard
Facial recognition	ISO/IEC 19794-5
Fingerprint recognition	ISO/IEC 19794-4
Iris recognition	ISO/IEC 19794-6
Contactless ICs used in eMRTDs	ISO/IEC 14443 and ISO/IEC 7816-4
eMRTD testing	ISO/IEC 18745-1, ISO/IEC 18745-2, ISO/IEC 18745-3, ISO/IEC 18745-4

9. References

Airports Council International (ACI). (2021). *Airports invest in technology to advance industry recovery*. Retrieved from https://aci.aero/2021/03/11/airports-invest-in-technology-to-advance-industry-recovery/

Alaa S., A.-W., Qahwaji, R., Ipson, S., & Al-Fahdawi, S. (2017). *A multi-biometric iris recognition system based on a deep learning approach.*

Al-Ani, M. S., & Rajab, M. A. (2013). Biometrics Hand Geometry Using Discrete Cosine Transform (DCT). *Science and Technology*.

Alonso-Fernandez, F., Bigun, J., Fierrez, J., Fronthaler, H., Kollreider, K., & Ortega-Garcia, J. (2009). *Chapter 4: Fingerprint Recognition.*

Belhadj, F. (2017). *Biometric systemfor identification and authentication.*

Biometrics Research Group, Inc. . (2014). *Explainer: Palm print recognition*. Retrieved from Biometrics Research Group, Inc. : https://www.biometricupdate.com/201408/explainer-palm-print-recognition

Brown, D. (2018). *INVESTIGATING COMBINATIONS OF FEATURE EXTRACTION AND CLASSIFICATION FOR IMPROVED IMAGE-BASED MULTIMODAL BIOMETRIC SYSTEMS AT THE FEATURE LEVEL.*

Cavoukian, A. (2011). *Privacy by Design The 7 Foundational Principles .*

Committee of Experts. (2017). *WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA.*

Dhiman, A., Gupta, K., & Sharma, D. K. (2021). Chapter 1 - An introduction to deep learning applications in biometric recognition. In A. Dhiman, K. Gupta, & D. K. Sharma, *Trends in Deep Learning Methodologies.*

Duta, N. (2009). A survey of biometric technology based on hand shape. *Pattern Recognition*.

ICAO. (2015). Doc 9309 - Machine Readable Travel Documents.

ICAO. (2017). Doc 8973 - Restricted. *Aviation Security Manual* .

ICAO. (2020). Guiding Core Principles for the Development of Digital Travel Credential (DTC).

IDEMIA. (2021). *Biometrics on the rise: a surge in the use of iris recognition technology*. Retrieved from https://www.idemia.com/news/biometrics-rise-surge-use-iris-recognition-technology-2021-07-26

International Air Transport Association. (2020). Interoperability in the One ID Ecosystem - Technology Guidance.

International Air Transport Association. (2021). *Global Passenger Survey 2021.*

International Airport Review. (2022). *CONTACTLESS TECHNOLOGIES.*

International Civil Aviation Organization. (2007). MACHINE READABLE TRAVEL DOCUMENTS (MRTDs): HISTORY, INTEROPERABILITY, AND IMPLEMENTATION. Retrieved from https://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-17/TagMrtd17_WP016.pdf

International Civil Aviation Organization. (2022). ICAO 41st Assembly Agenda Item 13: Facilitation Programmes: PRE-TRAVEL VERIFICATION AND DIGITIZATION OF PROCESSES working paper. Retrieved from International Civil Aviation Organization: https://www.icao.int/Meetings/a41/Documents/WP/wp_081_en.pdf

Jain, A. K., Ross, A., & Prabhakar, S. (2004). *An introduction to biometric recognition.* Institute of Electrical and Electronics Engineers.

Jain, A., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*.

Majekodunmi, T. O., & Idachaba, F. (2011). *A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies.*

Ministry of Civil Aviation, India. (2018). "DIGI YATRA" REIMAGINING AIR TRAVEL IN INDIA. Retrieved from https://www.civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf

Ministry of Civil Aviation, India. (2018). Digi Yatra Policy. Retrieved from https://www.civilaviation.gov.in/sites/default/files/Digi%20yatra%20policy%20doc.pdf

MLIT Japan Civil Aviation Bureau. (2020). Guidebook on personal data management in One ID service at the Airports. Retrieved from https://www.mlit.go.jp/report/press/content/001332966.pdf

National Cyber Security Centre. (2019). *Biometric recognition and authentication systems*. Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/collection/biometrics/fingerprint

NEC. (2022). *NEC*. Retrieved from Advantages and Disadvantages of Fingerprint Recognition: https://www.nec.co.nz/market-leadership/publications-media/advantages-and-disadvantages-of-fingerprint-recognition/

Pandey, M., Yadav, R., & Pandey, A. (2020). S.H.A.D.E: System for Human Authentication in Dynamic Environment. *International Journal of Engineering Research & Technology (IJERT)*.

Raimugia, V., Patel, N., Pawar, A., & Deulkar, K. (2014). *Feature Extraction Techniques for Palmprint Identification: A Survey.*

Ross, A., & Jain, A. K. (2007). Human Recognition Using Biometrics: An Overview. *Annals of Telecommunications*.

Sabhanayagam, T., Venkatesan, V. P., & Senthamaraikannan, K. (2018). A Comprehensive Survey on Various Biometric Systems. *International Journal of Applied Engineering Research*.

Shen, C., Yu, S., Wang, J., & Hua, G. Q. (2022). *A Comprehensive Survey on Deep Gait Recognition: Algorithms, Datasets and Challenges.*

Singapore Immigration & Checkpoints Authority. (2020). *Use Of Iris And Facial Biometrics As The Primary Biometric Identifiers For Immigration Clearance At All Checkpoints*. Retrieved from https://www.ica.gov.sg/news-and-publications/newsroom/media-release/use-of-iris-and-facial-biometrics-as-the-primary-biometric-identifiers-for-immigration-clearance-at-all-checkpoints

Singpass. (n.d.). *Singpass*. Retrieved from https://www.singpass.gov.sg/main/

SITA. (2021). *Air Transport IT Insights 2021.*

Types of Biometrics – Hand Geometry. (2022). Retrieved from Biometrics Institute: https://www.biometricsinstitute.org/types-of-biometrics-hand-geometry/

Types of Biometrics: Finger Geometry – Key Considerations. (2022). Retrieved from Biometrics Institute: https://www.biometricsinstitute.org/types-of-biometrics-fingerprint-geometry-key-considerations/

Ungureanu, A.-S., Salahuddin, S., & Corcoran, P. (2020). *Towards Unconstrained Palmprint Recognition on Consumer Devices: a Literature Review.*

World Wide Web Consortium. (2022). *Verifiable Credentials Data Model v1.1*. Retrieved from https://www.w3.org/TR/vc-data-model/

Zhang, D., Yue, F., & Zuo, W. (2011). Palmprint Recognition. In D. Zhang, F. Yue, & W. Zuo, *Encyclopedia of Cryptography and Security.*