Cycle 2

Data and Technology Proof of Concept (PoC)

Use Cases

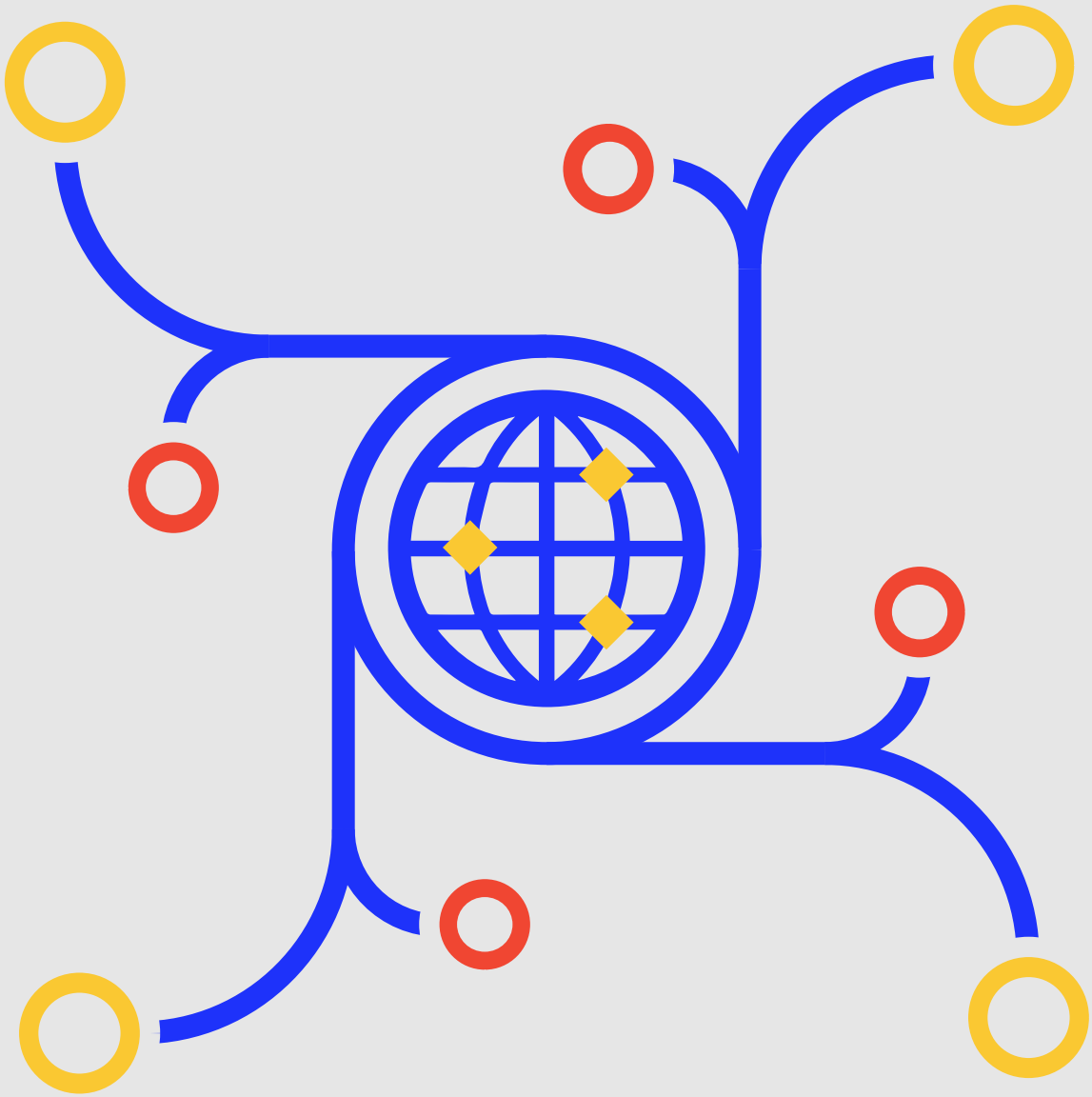


Table of contents

Use Case 1 3

IAG and British Airways, with Amadeus, NEC, Apple and Google Wallets

Seamless Digital Identity Enabled Interline Journey

(LHR–HND via HKG and with JAL)

Use Case 2 5

Japan Airlines, with Branchspace, NEC, SICPA, Hopae, and Face Express Wallet

Seamless Digital Identity Enabled Interline Journey

(HND–DOH via HKG and with Qatar Airways)

Use Case 3 7

Japan Airlines, with Amadeus, NEC and Google Wallet

Seamless Digital Identity Enabled Interline Journey

(HND–LHR via HKG and with BA)

Use Case 4 9

Japan Airlines, with NEC and Google Wallet

Seamless Digital Identity Enabled Return Journey

(HND–HKG)

Use Case 5 10

Air New Zealand

Seamless Digital Identity Enabled Journey

(AKL–HKG–AKL)

Use Case 6 12

IndiGo Airline, Bangalore Airport with Digi Yatra and SITA

Use Case 1

IAG and British Airways, with Amadeus, NEC, Apple and Google Wallets

Seamless Digital Identity Enabled Interline Journey

(LHR–HND via HKG and with JAL)

1. Objective of the Proof of Concept

This Proof of Concept demonstrates an end-to-end, interoperable digital identity journey across multiple airlines, airports, and jurisdictions, using standards-based digital identity credentials stored in the Apple and Google Wallets.

The PoC validates that a passenger can complete a seamless, biometric-enabled journey from Heathrow to Haneda via Hong Kong, inter-airline between British Airways and Japan Airlines, without repeated document presentation, while maintaining regulatory compliance and airline operational integrity.

The core objective is not a one-off pilot, but to prove a scalable, standards-driven identity architecture that can be reused across journeys, partners, and geographies.

2. Journey Scope and Flow

The PoC covers the following journey stages:

Airlines

- British Airways (operating carrier ex-LHR)
- Japan Airlines (interline partner ex-HKG)

Airports

- London Heathrow (LHR)
- Hong Kong International Airport (HKG)
- Tokyo Haneda (HND)

Journey Segments

- Origin check-in and biometric boarding at Heathrow
- Connection processing at Hong Kong
- Biometric boarding onto Japan Airlines at Hong Kong
- Biometric boarding onto British Airways at Hong Kong

The journey explicitly demonstrates interoperability across:

- Airlines
- Airport operators
- Biometric vendors
- Digital identity wallet providers
- Identity verification endpoints

3. Digital Identity and Credential Scope

The PoC uses a standards-compliant ISO23220 photoid credential stored in Apple & Google Wallet, shared securely and selectively with authorised verifiers.

Credential Characteristics

- Photo ID derived from a trusted document source
- Stored in consumer wallet (Apple & Google Wallet)
- Shared using ISO 18013-5 compliant protocols
- Used solely for identity verification purposes, not document replacement

Key Principle

The passenger remains in control of credential sharing. Credentials are presented via proximity-based or remote flows depending on journey stage.

4. Check-in and Pre-Travel Processing (In Scope)

At check-in via the British Airways mobile application:

- Passenger completes check-in using the BA iOS app
- Travel readiness checks are performed using the Amadeus Travel Ready web application, with passport data retrieval from Apple & Google Wallet
- Passenger is informed of contactless travel eligibility
- Consent is obtained for biometric enrolment and sharing

Biometric Enrolment

- As part of the British Airways branded, Amadeus Travel Ready web application, this checks the Airport touchpoint eligibility and retrieves the Hong Kong URL end-point from the IATA Contactless Directory
- Amadeus triggers the Hong Kong URL Allowing Hong Kong airport to issue a presentation request directly to the Apple and Google Wallet
- Upon traveller's consent, the Apple & Google Wallet performs the biometric enrolment to IDMS platform
- Remote enrolment uses OpenID4VP over DC API or ISO 18013-7 standards depending on the wallet
- Secure, direct Wallet-to-Verifier transfer is used
- No raw biometric data is shared between airlines

This establishes the passenger's biometric identity once, upstream of the journey.

5. Heathrow Boarding (Proximity-Based Flow)

At Heathrow Terminal 5:

- Passenger taps their iPhone or Android device at an NFC-enabled Biopod boarding gate
- The Photo ID credential is shared from Apple or Google Wallet to the verifier endpoint
- Biopod captures a live facial image
- A local 1:1 biometric match is performed between live capture and the Photo ID credential

Post-Match Actions

- Boarding authorisation request is sent to the BA DCS
- Passenger boards without presenting a physical passport or boarding pass

Key Validation

- Local biometric matching at the edge
- No centralised biometric database
- Airline control of boarding decision remains unchanged

6. Transit and Interline Boarding at Hong Kong

At Hong Kong International Airport, the PoC demonstrates a remote matching and interoperability model.

Remote Enrolment

- IDMS is populated at check-in time
- Credential sharing uses Wallet-to-Verifier flows
- Identity data is linked to the passenger's interline journey

Connections and Boarding

- Passenger approaches biometric eGates for connections and JAL boarding
- Live facial capture is performed at the gate
- A 1:n biometric match is executed against IDMS
- Boarding pass associated with the biometric profile is retrieved
- Passenger passes security, completes connection, and boards JL026

Key Validation

- Interline biometric continuity across carriers
- No re-enrolment required
- Airline separation of systems maintained

7. Standards and Interoperability (Explicitly In Scope)

The PoC validates adherence to global standards:

- ISO23220 (Photo ID)
- ISO 18013-5
- ISO 18013-7 (Remote identity presentation)
- OpenID4VP over DC API (Wallet to Verifier exchanges)
- Airline DCS and airport gate interoperability

This is a deliberate test of ecosystem readiness, not bespoke integration.

8. What This PoC Proves

The PoC explicitly demonstrates:

- Passenger-controlled digital identity can be used operationally at scale
- Biometric journeys can work across airlines and borders
- Interlining does not require identity re-capture or duplication
- Airlines retain operational and regulatory control
- Identity platforms can be reused across journeys and partners
- 1:1 and 1:n biometric matching compatibility

Use Case 2

Japan Airlines, with Branchspace, NEC, SICPA, Hopae, and Face Express Wallet

Seamless Digital Identity Enabled Interline Journey (HND–LHR via HKG and with BA)

1. Objective of the Proof of Concept

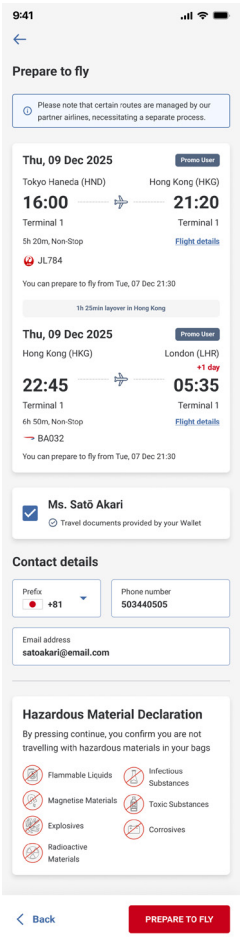
In this contactless travel proof of concept (PoC), the digital ID ecosystem covers two areas: Retail and Delivery. Specifically, the PoC demonstrates the entire travel flow where customers book airline tickets through personalized offers provided based on passport VC information, manage their orders, and experience a seamless and biometric-enabled journey from Haneda to London Heathrow via Hong Kong.

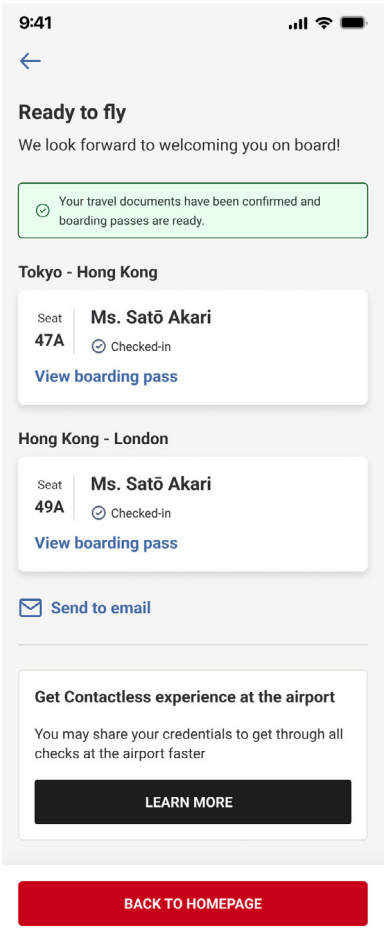
The primary objective of this PoC is to showcase an interline journey (Inter Airline Through Check-in: aka IATCI) utilizing ISO mDOC digital credentials formats and presentation across multiple airports and airlines, demonstrating real-world interoperability of digital identity standards. The traveller profile will be of Japanese citizen.

The passenger-facing interface illustrated in the JAL application and the Face Express Wallet is intentionally designed to align with the principles of the IATA Modern Airline Retailing (MAR) Offers & Orders framework. This approach enables the proof of concept to demonstrate forward compatibility with emerging retailing models in the industry.

Offers and Orders representation

- JAL assumes the role of the **retailing airline**, while Qatar assumes the role of the **supplying airline**
- The **Order** is treated as a single source of content, encompassing flight segments and ancillary services/ products associated with both carriers





2. Journey Scope

The PoC covers the following journey stages:

Airlines

- Japan Airlines (JL)
- British Airways (BA)

Airports

- Tokyo International Airport (HND)
- Hong Kong International Airport (HKG)
- London Heathrow Airport (LHR)

Passenger profile

- Japanese Passport Holder
- Adult
- No frequent flyer member
- Android user

Assumption

- Downloaded Face Express Wallet but not created any credentials
- Downloaded JAL app
- In the airline Shopping flow, purchase the lounge access at HND and HKG as an ancillary service
- The passenger will be offered discount flight by the age which is selectively disclosed

3. Journey Flow

Shopping flow at home

- Passenger starts shopping flow at JAL app for HND-HKG-LHR
- JAL app prompts using digital identity wallet for the booking
- Passenger linked to Face Express wallet from JAL app
- Face Express wallet displays Passport Digital Certificate setup process
- Passenger scan Passport, read the chip and capture live face image to create credentials
- Passenger notified that credentials were verified successfully by JAL app
- JAL app shows several flights to LHR and the passenger chose it
- JAL app shows several fares and passenger chose the discount fare which is offered by the age that is selectively disclosed
- Passenger needs to input contact information manually, but passport information is auto filled
- JAL app offers service such as seats, lounge, priority baggage
- Passenger chose the seat and added lounge service for both HND and HKG
- Passenger will confirm the service items and complete the payment
- JAL app shows the shopping confirmation screen and notifies passengers that your admissibility check is done at that time, and the authority will make final confirmation 24 hours before the flight
- And notify passenger the Contactless Travel is available after ready to fly
- JAL app prompts to save order to the wallet and passenger will save it in Face express wallet

Prepare and Ready to fly at home

- Passenger notified from push notification that it's time to prepare to fly and send a link
- Passenger clicks the push notification and opens the JAL app
- Passenger shares the Order VC to retrieve the booking
- JAL app display the booking information and passenger will confirm it. (All information such as passport, contact information is auto filled)
- Final admissibly check will be done and JAL app prompts the contactless travel information
- Passenger linked to Face Express app and shows consent page of HND and HKG
- Passenger will confirm and present the credentials to both HND and HKG
- Passenger will be linked to the JAL app home screen

Boarding at HND

- Passenger arrive to HND and go directly to the security and pass the gate by biometrics (1:N)
- Passenger arrive to boarding gate and board by using biometrics (1:N)

Arrive and Boarding at HKG

- Passenger arrive to HKG and go directly to the transfer security and pass the gate by biometrics (1:N)
- Passneger arrive to boarding gate and board by using biometrics (1:N)

Arrive at LHR

- Nothing to do at LHR

Use Case 3

Japan Airlines, with Amadeus, NEC and Google Wallet

Seamless Digital Identity Enabled Interline Journey (HND–LHR via HKG and with BA)

1. Objective of the Proof of Concept

The contactless travel Proof of Concept (PoC) demonstrates how digital identity ecosystems enable seamless travel from Haneda to London via Hong Kong. Travelers use digital wallets to store and share verifiable credentials including e-passports. By presenting these credentials to relying parties (airlines and airports), the system enables digital travel admissibility checks and contactless passage through airport touchpoints which includes security screening and boarding gates. For dynamic discovery of airport capabilities and its touchpoints along with checking passenger eligibility before sharing credential with relying parties (airports) an integration with IATA Contactless Travel Directory will be done.

The primary objective of this PoC is to showcase an interline journey utilizing ISO mDOC digital credentials formats and presentation across multiple airports and airlines, demonstrating real-world interoperability of digital identity standards. The traveller profile will be of UK citizen.

2. Journey Scope

The PoC covers the following journey stages:

Airlines

- Japan Airlines (JL)
- British Airways (BA)

Airports

- Tokyo International Airport (HND)
- Hong Kong International Airport (HKG)
- London Heathrow Airport (LHR)

Passenger profile

- UK Passport Holder
- Adult
- No frequent flyer member
- Android user

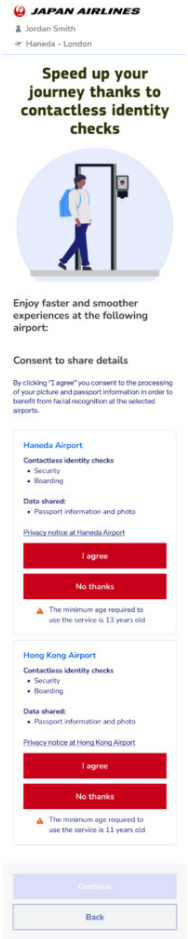
Assumption

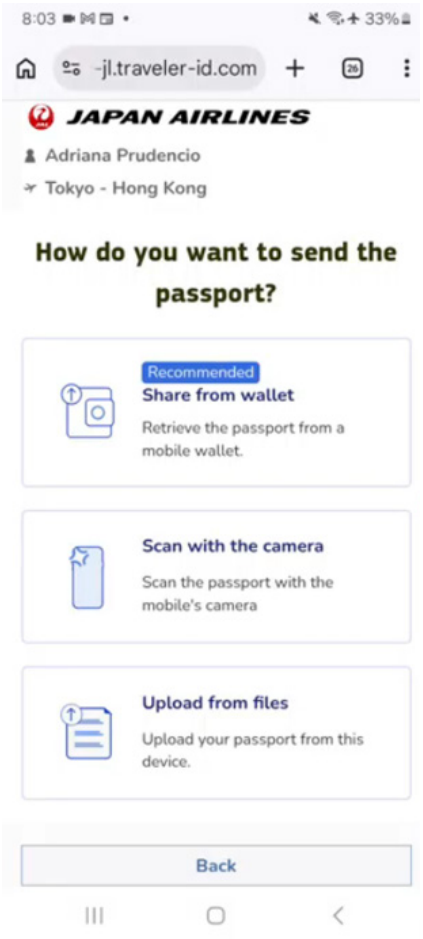
- Having e-passport copy at Google Wallet
- Having booking for HND-HKG-LHR with JL and BA flights
- Starts from the current check in and booking is retrived

3. Journey Flow

Check in flow at home

- Passenger open the web and prepare for flight
- Web app will prompt to verify the passport, and passenger chose share from wallet
- Passenger will make a consent to share credentials
- Document information will auto fill and admissibility check will be done
- Passenger will choose the seat for both flights
- Before the check in will complete, web app will prompt the contactless travel information that where the passenger could use the contactless travel
- Firstly, Passenger will agree for HND and pop up HND's web page
- HND's web page will request to share the credentials and passenger will confirm it
- Secondly, Passenger will agree for HKG and pop up HKG's web page
- HKG's web page will request to share the credentials and passenger will confirm it
- Web app will display that passenger is ready to have contactless travel experience at HND and HKG
- Check in is done and boarding pass is display
- Web app will shows the review consent button to revoke the consent from the booking home screen





Boarding at HND

- Passenger arrive to HND and go directly to the security and pass the gate by biometrics (1:N)
- Passenger arrive to boarding gate and board by using biometrics (1:N)

Arrive and Boarding at HKG

- Passenger arrive to HKG and go directly to the transfer security and pass the gate by biometrics (1:N)
- Passenger arrive to boarding gate and board by using biometrics (1:N)

Arrive at LHR

- Nothing to do at LHR

Use Case 4

Japan Airlines, with NEC and Google Wallet

Seamless Digital Identity Enabled Return Journey (HND–HKG)

1. Objective of the Proof of Concept

The contactless travel Proof of Concept (PoC) demonstrates how digital identity ecosystems enable seamless travel from Haneda to London via Hong Kong. Travelers use digital wallets to store and share verifiable credentials including e-passports. By presenting these credentials to relying parties (airlines and airports), the system enables digital travel admissibility checks and contactless passage through airport touchpoints which includes security screening and boarding gates. For dynamic discovery of airport capabilities and its touchpoints along with checking passenger eligibility before sharing credential with relying parties (airports) an integration with IATA Contactless Travel Directory will be done.

The primary objective of this PoC is to showcase an interline journey utilizing ISO mDOC digital credentials formats and presentation across multiple airports and airlines, demonstrating real-world interoperability of digital identity standards. The traveller profile will be of UK citizen.

2. Journey Scope

The PoC covers the following journey stages:

Airlines

- Japan Airlines (JL)

Airports

- Tokyo International Airport (HND)
- Hong Kong International Airport (HKG)

Passenger profile

- US Passport Holder
- Adult
- No frequent flyer member
- Android user

Assumption

- Having e-passport copy at Google Wallet
- Having booking for HND-HKG HKG-HND with JL flights
- Starts from the current check in and booking is retrived

3. Journey Flow

Check in flow at home

- Passenger starts the flow from the check in complete
- Passenger clicks the save to wallet the boarding pass
- Google Wallet will show up and passenger will confirm to use the contactless experience
- Passenger will make a consent to both HND and HKG to share credentials
- Credentials will be shared on passenger consent

Boarding at HND

- Passenger arrive to HND and go directly to the security and pass the gate by biometrics (1:N)
- Passenger arrive to boarding gate and board by using biometrics (1:N)

Arrive and Boarding at HKG

- Passenger arrive to HKG and go directly to the security and pass the gate by biometrics (1:N)
- Passenger arrive to boarding gate and board by using biometrics (1:N)

Use Case 5

Air New Zealand

Seamless Digital Identity Enabled Journey (AKL–HKG–AKL)

1. Objective of the Proof of Concept

This Proof of Concept demonstrates how Air New Zealand participates in a standards-based digital identity ecosystem to enable a more seamless, privacy-preserving travel journey across airline, airport and government touchpoints.

The PoC validates:

- Use of verified digital identity attributes derived from a traveller's passport
- Selected contactless processing at airport touchpoints
- Secure, consent-based data sharing to support offshore transit processing
- Integration with New Zealand border processes on return, under the authority of the New Zealand Customs Service

2. Journey Scope and Flow

Airline

- Air New Zealand (NZ)

Airports

- Auckland International Airport (AKL)
- Hong Kong International Airport (HKG)

Passenger profile

- Single traveller
- New Zealand passport holder
- Air New Zealand Mobile app user with Air New Zealand digital identity created

3. Digital Identity and Credential Scope

The PoC uses verified identity attributes derived from a New Zealand ePassport and held by the traveller in a digital identity wallet.

In scope

- Passport-derived identity attributes
- Boarding pass data where required for operational processing
- New Zealand Traveller Declaration traveller contact information (return journey only)

Key principles

- Traveller consent governs all data sharing
- Only the minimum data required is disclosed at each step
- Identity and biometric data are handled in accordance with defined purpose, consent and retention controls

4. Pre-Travel Preparation and Check-in (Outward Journey)

Digital identity setup

- The traveller sets up or confirms their digital identity within the Air New Zealand app
- Verified digital identity attributes derived from a New Zealand ePassport are established once and made available for use across the journey, subject to traveller consent

Pre-travel preparation

- The traveller adds passport information to their booking using their digital identity wallet
- Travel readiness checks can be performed by the traveller using verified digital identity attributes retrieved from their digital identity, via IATA-standard travel readiness APIs

Online Check-in

- The traveller is informed of eligible contactless touchpoints at Auckland and Hong Kong airports
- During online check-in, the traveller provides explicit consent, per touchpoint, to share verified digital identity attributes from their digital identity wallet with Air New Zealand and eligible airport touchpoints, in order to enrol into seamless travel and complete check-in processing

5. Auckland Airport – Departure Lounge Access

Biometric lounge access on departure is included as an Auckland touchpoint within the Proof of Concept.

- The traveller proceeds to the Air New Zealand lounge at Auckland Airport prior to departure
- Identity is verified using a 1:N biometric match against the traveller's verified digital identity
- The traveller's lounge eligibility is confirmed

6. Departure from Hong Kong International Airport

Departure from Hong Kong International Airport is included as a key scenario for validating interoperability within the Proof of Concept.

- The traveller departs from HKG on an international flight included within the PoC scope
- Air New Zealand integrates with Hong Kong International Airport's Flight Token system to enable contactless processing at selected departure touchpoints
- Facial recognition is used at those Hong Kong airport touchpoints, based on traveller consent provided prior to travel
- Identity verification at departure does not require re-enrolment where the traveller has already established their digital identity through the approved PoC process

The HKG departure scenario is included to validate that a standards-based digital identity approach can interoperate with Hong Kong International Airport's Flight Token system to support contactless departure processing, while maintaining traveller consent, data minimisation and reuse of prior identity verification.

7. Return Journey – Entry into New Zealand (NZ Customs Integration)

On the inbound journey to New Zealand, the PoC validates support for pre-arrival and arrival border processes, under the authority of the New Zealand Customs Service.

New Zealand Traveller Declaration

- The traveller completes the New Zealand Traveller Declaration digitally prior to arrival
- Passport and flight data required for the declaration are provided from verified identity attributes
- Data is disclosed to the New Zealand Customs Service strictly for border processing purposes, based on explicit traveller consent, using the digital New Zealand Traveller Declaration provided by NZ Customs

Border processing

- The New Zealand Customs Service acts as the verifier and retains full decision-making authority
- The PoC does not replace physical passport requirements or existing border control processes

8. Standards and Interoperability

The PoC aligns with:

- ISO-based digital identity and mobile document standards
- OpenID-based verifiable credential issuance and presentation
- IATA Contactless Travel and interoperability principles

No proprietary or airline-specific identity formats are required.

9. Issuer, Verifier and Directory Context (High-level)

- **Issuer:** Air New Zealand issues verified identity attributes derived from the traveller's passport into the traveller's digital identity wallet
- **Airline verifier:** Air New Zealand verifies selective identity attributes during booking, pre-travel preparation and check-in
- **Airport verifier:** Hong Kong International Airport verifies identity for biometric transit processing
- **Government verifier:** The New Zealand Customs Service verifies traveller information for inbound border processing
- **IATA Contactless Travel Directory:** Used to discover contactless capabilities and to assess passenger eligibility and trust requirements across the journey

10. What This PoC Demonstrates for Air New Zealand

This Proof of Concept demonstrates that Air New Zealand can:

- Participate in a globally interoperable digital identity ecosystem
- Support interoperable airport processing through integration with Hong Kong International Airport's Flight Token system
- Support offshore airport processing without centralising biometric data
- Enable secure, consent-based data sharing with border authorities
- Establish a scalable foundation for future partner and network expansion

Use Case 6

IndiGo Airline, Bangalore Airport with Digi Yatra and SITA

1. Primary Objective and Value Proposition

In this contactless travel proof of concept (PoC), demonstrates the entire travel flow where passengers book airline tickets, based on passport information, manage their travel bookings, and experience a seamless and biometric-enabled journey from Bengaluru to Doha.

The primary objective of this PoC is to showcase the passenger journey (Through Airport Entry and Boarding) utilizing ISO mDOC digital credentials formats and presentation across multiple airports and airlines, demonstrating real-world interoperability of digital identity standards. The traveller profile will be of Indian citizen.

Below are the key points and value proposition of the PoC:

- Enable a standards-based, consented, privacy-preserving digital travel experience where Digi Yatra (DY) Wallet acts both as Holder wallet and as Issuer of ISO mDOC (Photo ID) derived from the traveler's chip ePassport
- Passenger makes a booking through the IndiGo App, with all the necessary credentials and makes the payment. The passenger then moves forward to Web check-in, IndiGo shares the boarding pass (BP) to the DY app via secure app intent-based integration between IndiGo and Digi Yatra Application; DY issues a Boarding Pass Verifiable Credential (BP VC) in SD-JWT format
- As a second use case to demonstrate interoperability, SITA Issuer issues VC to SITA Wallet and then hand over to BLR Verifier
- BLR Airport acts as Verifier to validate the BP VC and the passport portrait image; minimal necessary data is consumed and stored in local IDMS strictly for day-of-travel validations at Entry, Security, and Boarding. IDMS (SITA SmartPath) enhanced to interface with DYCE enabling intimation to passenger on successful use of VC and offer revoke on demand
- In India, the journey begins at Entry: passenger completes 1:N facial validation; upon successful match, BP details are validated against AODB for flight status and if flight status matches, it is then validated with DCS, to allow access if DCS data matches the BP details
- For this POC, Digi Yatra Foundation's SSI trust ecosystem and credential lifecycle (for Issuer, Holder and Verifier) was upgraded for global standards and interoperability profile using open-source platform from **Linux Foundation Decentralized Trust project CREDEBL**
- IATA Travel Directory is used to discover verifier URLs and contactless services at airports
- Airport purges day-of-travel data within 24 hours after flight's scheduled departure
- Passenger can also purge the data on demand by choosing Revoke consent from Digi yatra Application

2. Participants, Roles and Responsibilities

- **Traveler (Indian national):** Consents to issuance and sharing; uses DY Wallet as Holder
- **Digi Yatra Wallet (DY App):** (a) Issues ISO mDOC (Photo ID format) from chip ePassport (on-device NFC read); (b) Holds mDOC and BP VC; (c) Issues BP VC (SD-JWT) from IndiGo BP payload; (d) Presents credentials to airport verifiers with selective disclosure
- **IndiGo (6E):** Completes web check-in process issues boarding pass in the 6E app; triggers app intent to share BP payload to DY; authoritative source for reservation status (Ready-to-Fly) during validations
- **BLR Airport (BIAL):** Verifier for BP VC and live biometric at Entry, Security, and Boarding; consumes minimal data into local IDMS for day-of-travel continuity; Deploys infrastructure (Egate, Camera and Facial Recognition software) and AODB and DCS integration with Airline to validate; purges within 24 hours of flight's scheduled departure
- **IATA Travel Directory:** Discovery layer for verifier endpoints and airport contactless services
- **Additional scenario with SITA Wallet (SITA App):** Issues ISO Buffer (Photo ID) from chip ePassport (b) Holds ID and BP VC (c) Handover VC to Digi Yatra ecosystem for presentation to airport verifiers. App allows selective disclosure by passenger to use ID in SITA App or with DY App

3. Journey Scope & Routes Covered

Airline

- IndiGo Airlines (6E)

Wallet

- Digi Yatra
- SITA

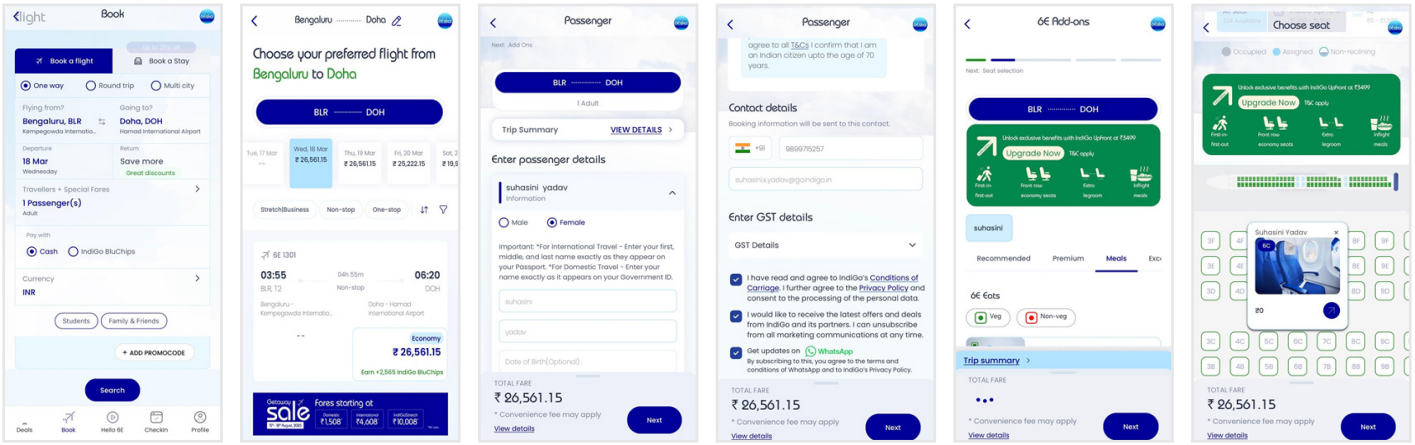
Passenger profile

- Adult Indian Passport Holder (only ePassport)
- No frequent flyer member
- Digi Yatra User
- Android/iOS user

4. End-to-End Process Flow (High Level)

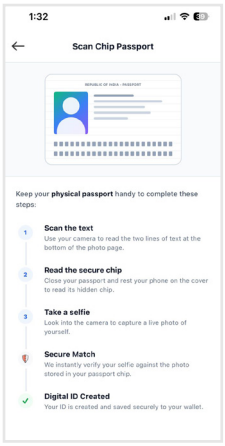
Booking, Web Check-in and Sharing BP with DY (6E and DY Application)

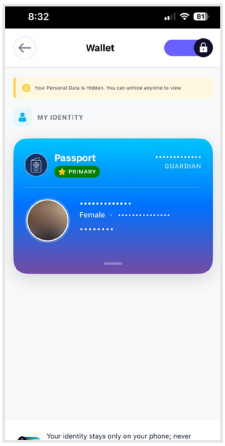
- Passenger makes a booking through 6E application from BLR to DOH
- 6E App shows several flights to DOH for the passenger to choose from
- 6E app shows multiple fares for the passenger to choose from, basis the age that is selected and disclosed
- 6E app offers ancillary services such as meals, seats, lounge, priority baggage, Fast forward
- Passenger will confirm the service items and complete the payment
- 6E app prompts entering passenger's Passport credentials for Web Check-in process
- Passenger notified that credentials were verified successfully by 6E app
  (Backend Validation through Timatic & IATA Contactless Travel Directory)
- Once the passenger is verified, Boarding pass is issued to the passenger
- The app also displays a notification for passenger reflecting whether Contactless Travel is available for the sector
- After passenger consents to the contactless journey Secure app intent transfers BP payload to DY app

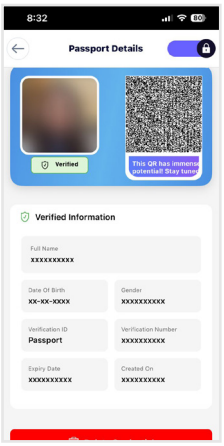


Onboarding/Credential Creation (In Digi Yatra Application)

- It is prerequisite for passenger to complete these steps and create Passport Verifiable Credential in DY app
- Traveler opens DY app
- Performs MRZ Read followed by NFC chip read of ePassport
- DY issues mDOC (Photo ID) Credential
- User saves the Photo ID credential into wallet (issuer = DY)

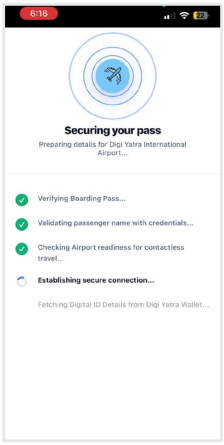


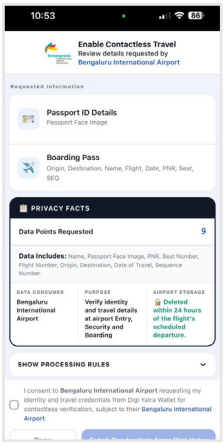


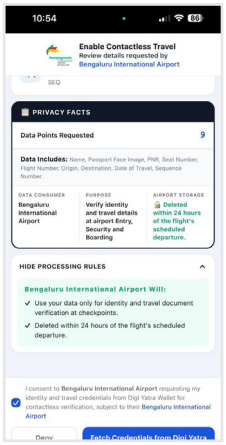


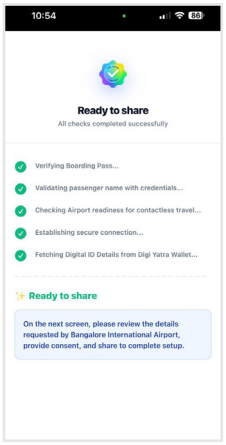
Sharing Boarding Pass and Photo ID VC with BLR Airport (Digi Yatra Application and Airport Verifier)

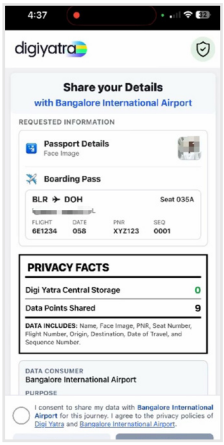
- DY App does basic control checks on the Boarding Pass (Name with VC name, Future Date, Origin, Destinations and Not an e-ticket)
- DY converts the BP payload to a Boarding Pass VC (SD-JWT)
- DY references IATA Contactless Travel Directory to discover BLR Verifier agent /services endpoints
- BLR Airport acts as Verifier to validate the BP and Photo ID VC
- On successful verification minimal necessary data is consumed and stored in local IDMS (Identity Management System) of airport, strictly for day-of-travel validations at Entry, Security, and Boarding
- Passengers can check the status of the Boarding Pass shared with Airport to ascertain if Boarding pass was successfully received and stored at the airport or not
- Passenger can also choose to revoke the consent and request for on demand deletion of data from Airport and opt out of the contactless journey. For this a new connectivity was established between Digi Yatra Ecosystem and Airport IDMS (SmartPath) to enable interactive capability

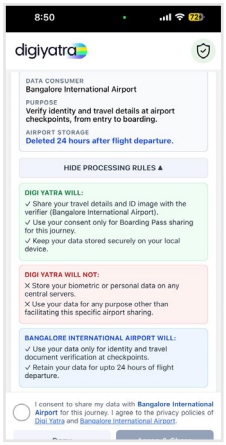


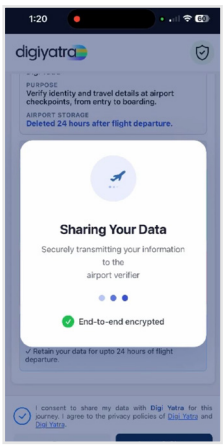


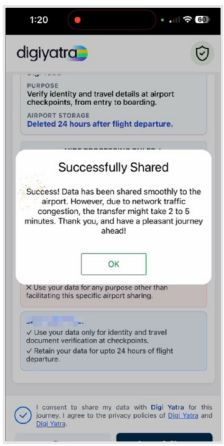


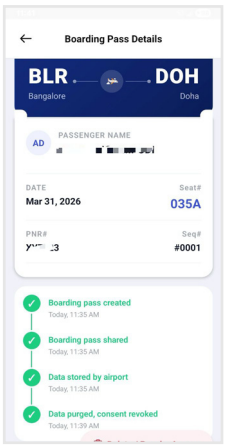












5. Day of Travel At-the-Airport

- Passenger touch points enabled for Digi Yatra are Entry (Basis AODB and DCS Integration), Security (SHA-Basis AODB and DCS Integration) and Boarding
- Each touchpoint performs live face 1:N against Photo ID face stored in BLR IDMS+ AODB and DCS validation before granting access
- BLR airport automatically purges the data within 24 hours after flight's scheduled departure
- Once Data is purged, Digi Yatra system is updated about the same, which in turn updates the status back to Passenger

6. Assumptions and Dependencies

- Downloaded 6E App
- Downloaded Digi Yatra App with valid passport credentials
- Passenger consents to share the data with DY & Airport
- BLR Airport equipped with IDMS + 1:N capability with e-gates at touch points
- BLR Airport touch points integrated with participating Airline AODB and DCS for Day of Travel Validations
- IATA Contactless Travel Directory entries published for BLR (verifier) and contactless travel status of the airport
- Immigration and Border Control touch points are not in scope of POC
- Passenger will be reporting at the check-in/Bag Drop counter to collect the physical boarding pass for Immigration and PESC clearance (Physical stamping requirements)

7. SITA App based Flow

Onboarding/Credential Creation (In SITA App)

- Traveler opens SITA App
- MRZ Read followed by NFC chip read of ePassport
- SITA issues Photo ID Credential
- User saves the Photo ID credential into wallet (issuer = SITA)

Sharing Boarding Pass and Photo ID VC with BLR Airport (SITA App and Airport Verifier)

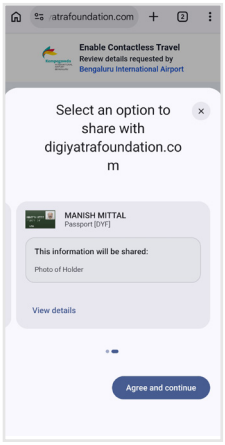
- SITA App does basic control checks on the Boarding Pass (Name with VC name, Future Date, Origin, Destinations and Not an e-ticket)
- SITA App scans Boarding Pass QR Code
- SITA App references IATA Contactless Travel Directory to discover BLR Verifier agent /services endpoints and handover VC to DigiYatra.
- DY acts as Verifier for BLR Airport to validate the BP and Photo ID VC
- On successful verification minimal necessary data is consumed and stored in local IDMS (Identity Management System) of airport, strictly for day-of-travel validations at Entry, Security, and Boarding

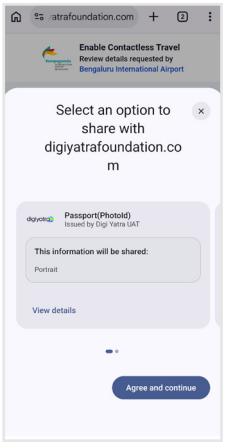
Day of Travel At-the-Airport

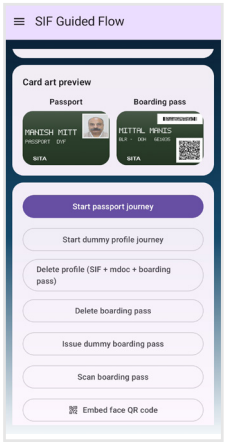
- Passenger touch points enabled for Digi Yatra are Entry (Basis AODB and DCS Integration), Security (SHA-Basis AODB and DCS Integration) and Boarding
- Each touchpoint performs live face 1:N against Photo ID face stored in BLR IDMS+ AODB and DCS validation before granting access
- BLR airport automatically purges the data within 24 hours of flight's scheduled departure

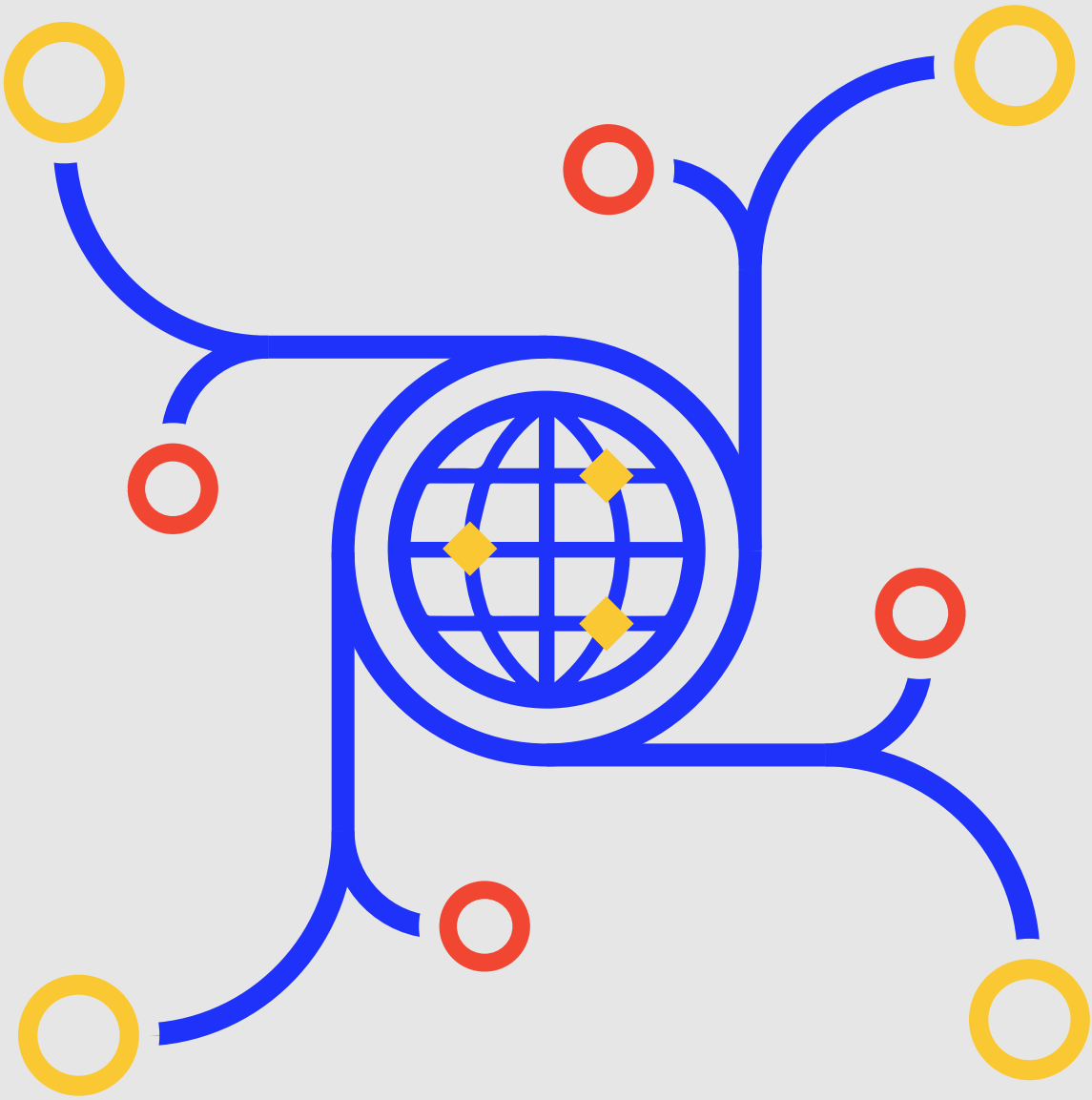
Assumptions and Dependencies

- SITA App installed on Android with valid passport credentials
- Passenger consents to share the data with DY & Airport
- BLR Airport equipped with IDMS + 1:N capability with e-gates at touch points
- BLR Airport touch points integrated with participating Airline AODB and DCS for Day of Travel Validations
- IATA Contactless Travel Directory entries published for DY (issuer), BLR (verifier) and contactless travel status of the airport
- Immigration and Border Control touch points not in scope of POC









International Air Transport Association
SS135-800 rue du Square-Victoria
Montreal, QC, H3C 0B4
Canada

iata.org