https://www.civilaviation.gov.in/

Version 7.5

4th March 2021

"DIGI YATRA BIOMETRIC BOARDING SYSTEM"

REIMAGINING AIR TRAVEL IN INDIA

सत्यमेव जयते

DIGI YATRA BIOMETRIC BOARDING SYSTEM

Ministry of Civil Aviation
Rajiv Gandhi Bhavan
New Delhi- 110003

TABLE OF CONTENTS

PREFACE

The Ministry of Civil Aviation (MoCA) of Government of India is responsible for formulation of national policies and programmes for the development and regulation of the Civil Aviation sector in the country. It is responsible for the administration of the Aircraft Act, 1934, Aircraft Rules, 1937 and various other legislations pertaining to the aviation sector in the country. The Indian civil aviation industry has emerged as one of the fastest growing industries in the country during the last three years. India is currently considered the third largest domestic civil aviation market in the world and is expected to become the world’s largest domestic civil aviation market in the next 10 to 15 years.

The Civil Aviation industry has therefore ushered in a new era of expansion, driven by factors such as low-cost carriers (LCCs), modern airports, Foreign Direct Investment (FDI) in domestic airlines, advanced information technology (IT) interventions and growing emphasis on regional connectivity.

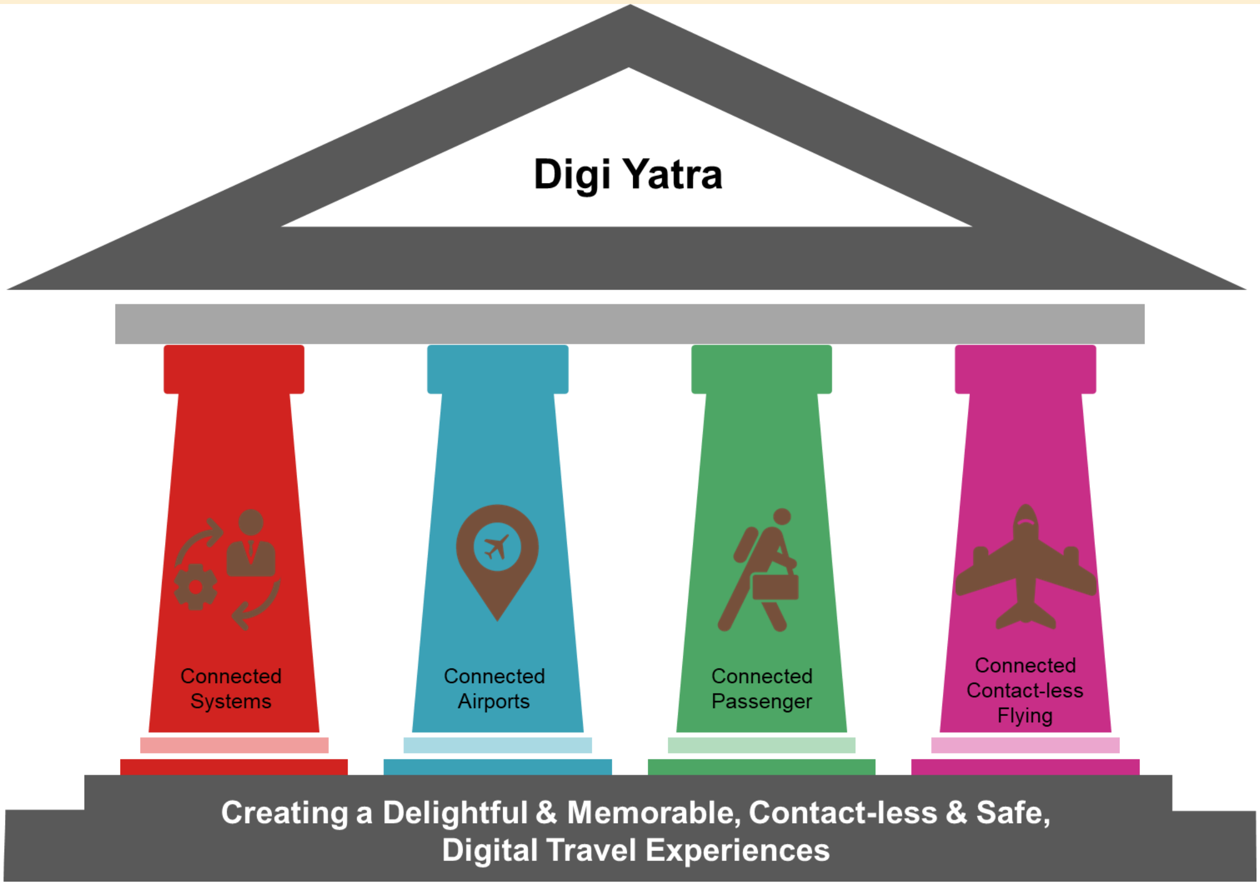
Considering the growth projections, its direct impact on the Passenger journey, the cost of Infrastructure and the impact on the speed and efficiency of Passenger processes, The Ministry of Civil Aviation has taken up a key initiative to reimagine air travel in India looking beyond the conventional “build a bigger Airport to manage more Passengers” to look for Innovation and technology for better and cost effective solutions. One of the key initiatives in this direction is “The Digi Yatra” which intends to give a seamless, contact-less, hassle-free and paperless journey experience to every air traveller in India. Using cutting edge Identity Management and “Face recognition” technologies, it aims to simplify the Passenger processes at various check points in the Airport right from the terminal entry gate, check-in/ bag drop, security check and boarding gates.

The MoCA, has constituted a Technical Working Committee (TWC) consisting of Subject Matter Experts (SME) from a few of the major airports in India and AAI. The TWC under the Digital Cell of Digi Yatra has been working for the past year on the Digi Yatra Project and have done trials at some of the leading airports in India to find out the best possible solution that can be implemented by all the airports in India. After several workshops and deliberations with aviation stakeholders and regulators, the Digi Yatra Process was documented by the TWC and submitted to MoCA for circulating as a National Policy.

Subsequent to the release of the policy and the issue of the CAR by the MoCA, there have been further deliberations held to make the enrolment process more user friendly and empowering passengers themselves to create the Digi Yatra ID credential. Passengers will also be able to directly share the Digi yatra-ID travel credential data to relevant stakeholders like Airlines, OTAs, Airports & other regulatory bodies.

With the new Digi Yatra process, Passengers will no longer need to show their tickets/ boarding passes and their physical Identity cards at many of the check points at the Airport, since the ticket/ boarding Pass is integrated with the Identity document. This will lead to reduced queue waiting times, faster processing times, Contact-less and safer and simpler processes.

DIGI YATRA VISION


Digi Yatra
Connected Systems
Connected Airports
Connected Passenger
Connected Contact-less Flying
Creating a Delightful & Memorable, Contact-less & Safe, Digital Travel Experiences

OBJECTIVES

Every passenger, (Indian citizens and foreigners) become a “Digi Yatri” and enjoys the privileges and benefits of the “Digi Yatra” Program. The main objectives are as below:

a. Enhance passenger experience and provide a simple and easy experience to all air travelers.
   i. Empower passengers to create their Digi Yatra ID Credentials
   ii. Deliver a seamless, paperless, Contact-less and hassle-free experience to all passengers across all processors/ Check-points at all Indian airports. (Including Tier-1, 2 and 3 airports)
   iii. Improve passenger experience and provide a safe and contact-less process and help passengers plan their trips efficiently.
   iv. Receive relevant information pertaining to various facilities, protocols, airline timings, queue waiting times at the airport.

b. Achieve better throughput through existing infrastructure using “Digital Framework”.
   i. Walk-through security scanners swiftly owing to advanced biometric security solutions.
   ii. Stay connected through the airport, possibly through airport Wi-Fi, engage in customized digital offerings at experience zones.

c. Result in lower cost operations.
   i. Remove redundancies at Checkpoints.
   ii. Enhance resource utilization.

d. Digitize current manual processes and to bring better efficiencies
   i. Get real time notifications about congestion & delays to have greater visibility on the next step of journey.
   ii. Navigate seamlessly through the airport using digital guidance systems, interactive kiosks and augmented reality apps.
   iii. Stay connected during flights and indulge in immersive experiences. Also book in-flight services and destination-based offerings digitally.

e. Enhance security standards and improve current system performance.
   i. Enhance security at Indian airports using “Digi Yatra ID” based Identification with real-time biometrics.
   ii. Validate Boarding pass or e-ticket with the airline system in real-time.
   iii. Use face biometric single token for processing Passengers at Checkpoints in the airport and also extend to Passengers without AADHAAR or Digi Yatra ID using biometric validation
   i. Phased rollout by all airports.

f. Rollout of “Digi Yatra” system with a digital “ID” backed by a strong verifiable government issued identity like AADHAAR, Driving License, Passport & others, enabling a seamless travel experience for Passengers at all airports across India.

GOALS

a. Set the standards & standard operating procedures (SOPs) for Digital Transformation of the Indian Aviation Industry
b. Create a common "Digi Yatra" Identity management eco-system with "Digital Identities" like AADHAAR, Driving License, Passport & Others, enabling Biometric Boarding Process for All Airports (Tier1, 2 & 3) across India
    i. The common Digi Yatra ecosystem will be built by a joint venture company (JVC) or special purpose vehicle (SPV) under the Section 8 of the companies act 2013 that has been established by the AAI and the five major airport operators in India.
c. Monitor and manage a time bound system rollout by all airlines, online travel agents, global distribution systems & airports
d. Conduct mass communication, marketing & awareness campaign for the new standards through social media, TV and newspapers.

TARGET AIRPORTS AND USERS

TARGET USERS

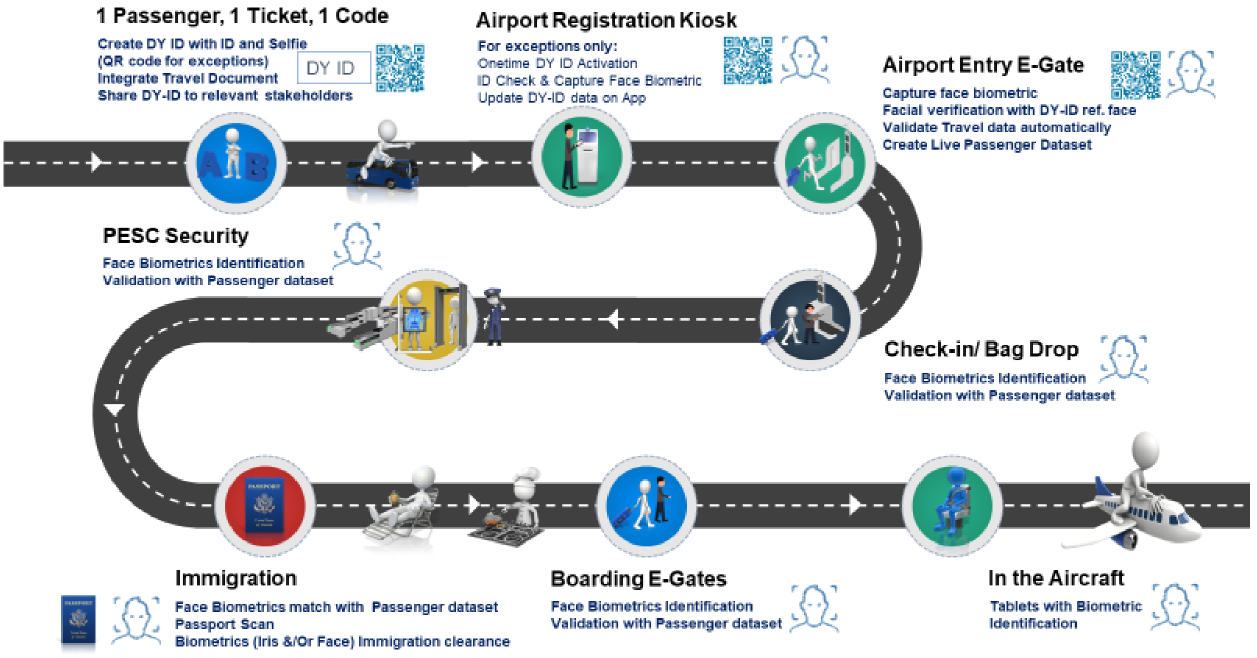
a. The new process shall cater to all Passengers at any airport in India, be it Indian citizens (With or without Digi Yatra ID) or foreign nationals
b. The process shall simplify & ease the Passenger process equally for different Passenger types
    i. First time and frequent flyers in India
    ii. Group travelers and families
    iii. Foreign citizens or tourists

THE “DIGI YATRA” CONCEPT & SUMMARY PROCESS

DIGI YATRA- ID TRAVEL CREDENTIAL & PASSENGER PROCESS BRIEF

Booking	Registration Kiosk (Exceptions only)	Entry Gate	Self Service Check-in / Bag Tags	Self Service Bag Drop or Assisted Bag Drop	PESC Entry	Departure Immigrations	Self Boarding gate
• DY-ID App Download • DY-ID Enrolment • Digital Identity Validation (GOI approved IDs) • (Optional) Update Passport data • Extract face from ID • Selfie Capture • Create DY-ID travel Credential • If selfie match is unsuccessful, Create a QR code for one-time manual ID validation by CISF • Update Travel data, App shares DY-ID profile with Airline, Airport & Immigration	• Scan QR code • Capture face • Show ID card to CISF • One time manual ID validation with CISF • CISF acceptance • Push the updated Face biometric and DY-ID	• (Optional) Scan Boarding pass • Match face with DY-ID reference face • Validate Boarding Pass • Create PAX dataset for the journey	• Match face • Validate Boarding Pass • [Check-in & Seat selection] • Print bag tag	• Match Face • Validate Boarding Pass • Deposit bag	• Match Face • Validate Boarding Pass • Enter PESC	• Match Face • Validate Boarding Pass • Validate Passport • Visa Check	• Match Face • Validate Boarding Pass • Enter boarding gate

THE DIGI YATRA JOURNEY: CONCEPT



1 Passenger, 1 Ticket, 1 Code

Create DY ID with ID and Selfie
(QR code for exceptions)
Integrate Travel Document
Share DY-ID to relevant stakeholders

Airport Registration Kiosk

For exceptions only:
Onetime DY ID Activation
ID Check & Capture Face Biometric
Update DY-ID data on App

Airport Entry E-Gate

Capture face biometric
Facial verification with DY-ID ref. face
Validate Travel data automatically
Create Live Passenger Dataset

PESC Security

Face Biometrics Identification
Validation with Passenger dataset

Check-in/ Bag Drop

Face Biometrics Identification
Validation with Passenger dataset

Immigration

Face Biometrics match with Passenger dataset
Passport Scan
Biometrics (Iris &/Or Face) Immigration clearance

Boarding E-Gates

Face Biometrics Identification
Validation with Passenger dataset

In the Aircraft

Tablets with Biometric Identification

DIGI YATRA ECOSYSTEM

DIGI YATRA ID TRAVEL

a. This Common Digi Yatra Ecosystem with its Central Ecosystem, Apps, Software Development Kits (SDK) will be built by a joint venture company (JVC) or special purpose vehicle (SPV) under Section 8 of the Companies Act 2013 is established by the AAI and all private airport operators.

b. The JVC/ SPV shall obtain the AUA/ KUA license from UIDAI (If needed) or subscribe to AADHAAR AUA/ KUA services from UIDAI's authorized agencies.

c. The Common Digi Yatra ID ecosystem offers core passenger services viz. enrolment, authentication, consented profile sharing etc., and shall be built as a shared national infrastructure (henceforth referred as "Digi Yatra Ecosystem") with APIs, Mobile Apps, SDKs & Website for airports, airlines and other stakeholders to integrate. The salient features of the process are as below.

   i. The primary service will be used at the airport terminal entry for the purpose of Identity Check using Digi Yatra ID Travel credentials with the single token of Face Biometrics.

   ii. Passengers would also have the ability to directly share their Digi Yatra ID Travel credentials to airports and other stakeholders

   iii. For passengers who do not opt for the Digi Yatra-ID registration, provision will be made to enroll at the airport

   iv. For passengers who do not wish to use facial biometric, provision will be made for automated travel document check (Using Barcode/ Mobile QR code scan) on e-gates with an ability for CISF security to do a manual ID Card check and permit passengers to enter the Airport Terminal and cross other check points inside the airport

   v. At all other check points across the airport Viz. Check-in / Bag-drop/ Self Service Bag Drop, Pre-embarkation Security Check (PESC) Security Check Entry, Boarding Gates, Lounges etc. the airport Digi Yatra Biometric Boarding system will use the Face biometric single token and/ or Barcode/ Mobile QR code for entry into the relevant areas, with appropriate reconciliation system at aircraft door.

      i. The subsequent phase will also include departure and arrival immigration Automated Border Control (ABC).

   vi. This service shall be provided to passengers and other stakeholders in the form of a Central Ecosystem/ Mobile App/ SDK integration by the Digi Yatra foundation.

   vii. As the primary and mandatory passenger check is at the Airport entry gate, the Digi Yatra ecosystem will provide the ability for a 1:1 authentication based on facial recognition, which will be progressively upgraded to a 1:N authentication for a superlative passenger experience by eliminating the need to scan the boarding pass at the entry e-gate.

viii. Enrolled passengers share a copy of Digi Yatra ID Travel Credential with a single token of face biometrics to local airport/s for temporary usage. This facial data cannot be stored by airports for longer than the duration of transit of passenger and facial data will be purged out of the system 24 hours after take-off/ departure of the flight.

ix. At the time of consent collection, Digi Yatra ecosystem/ App will strictly inform and take consent from the user for the sharing of face biometric data for the airport checkpoints and optionally another consent to opt for any value added services that the passenger may wish to avail from the Digi Yatra ecosystem partners.

x. Airports may be permitted to create profile of users based on explicit consent from the user for marketing/ sales/ promotional offers etc.

    i. This consent shall be taken independently as a separate consent during registration of Digi Yatra customers.

    ii. A one click opt-out link shall be made available to users directly on the App, as well as through the Digi Yatra ecosystem.

xi. Creation and use of the Digi Yatra ID Travel Credential by a passenger will be completely voluntary, and a one-time registration process using a Govt. ID is needed to enroll into the Digi Yatra Platform.

    i. Users will also have an option, at any time, to opt-out and delete their profile.

xii. In order to simplify the user experience and to encourage more passengers to use the Digi Yatra Ecosystem, a single stage self-service registration process using online ID verification, selfie based biometric enrolment and facial matching is envisaged for majority of the passengers.

    i. A second stage authentication is envisaged only for those who fail to get authentication using online process.

    ii. The single step registration consists of pre-registration activity and online verification of biographic data and facial matching of selfie with the image received from the ID data base such as AADHAAR, Driving License etc.

    iii. In case of any failure in the single stage registration or if the passenger is using an ID not supported for online verification, the authentication will be done through a manual process by CISF at the registration Kiosk at the airport.

xiii. The choice of Govt. ID used for enrolment is the choice of the passenger. Passengers can use any of the valid Government ID as per BCAS guidelines.

xiv. Passengers who have successfully enrolled once do not have to go to the Registration kiosks.

xv. For passengers who chose not to share biometric and to use the conventional process of Boarding Pass Barcode/ Mobile Boarding pass with QR code or Ticket with Barcode, the process will be semi-automated with Barcode/ Mobile QR code scan and a manual ID card check by CISF authorities at relevant checkpoints as necessary from the Airport entry to the Boarding gates.

d. From an UIDAI perspective, if necessary, the agency hosting the “Digi Yatra Ecosystem” will become a “Local Authentication User Agency AUA/ KUA” or subscribe to authentication services from UIDAI authorized AUA/ KUA agencies. This allows for AADHAAR authentication and e-KYC without having access to AADHAAR number.

i. It is important to note that no core biometric like iris/ fingerprints (or any other biometrics other than face) will be collected or stored anywhere in the system.

STEP 0 (A): DIGI YATRA ID TRAVEL CREDENTIAL: CREATION FROM AIRSEWA, AIRLINE/ OTA TICKET BOOKING SITE/ DY APP/ AIRPORT APP (USING AADHAAR)

a. Passenger downloads the AirSewa/Airline/ OTA/ Airport App and installs it on his/ her smartphone. The DY SDK will provide the registration interface to all applications.

b. Starts enrolment process by entering the following/ Scan the ID

   i. Name (First, Middle, Last name)

   ii. Mobile number

   iii. Email address

   iv. AADHAAR number/ Virtual AADHAAR Number

c. AADHAAR sends an OTP to the passenger's registered mobile number/ email id

d. Passenger enters the OTP received on the AADHAAR linked mobile number/ email id

e. AADHAAR then sends the e-KYC data to the passenger on the Digi Yatra ID App

f. **Optional:** Passport first page scan and e-passport reading with passport reference face

g. The Digi Yatra ID app extracts the reference face from this e-KYC data

h. Passenger is prompted to take a selfie with liveness detection and 3D image capture

i. The live face is matched with the reference face and if successful, the Digi Yatra ID travel credential is created.

   i. If the selfie match is not successful or if the Govt. of India issued ID is not supported with a digital database, then there is flag created and a Mobile QR code for a one-time physical Identity Document validation by the CISF at the airport

j. The Digi Yatra ID Travel credential is stored in the Digi Yatra App in a secure wallet in the smartphone

k. Passenger can now update the travel data by uploading the Ticket/ Boarding pass or by Scanning the electronic ticket (ETKT)/ Boarding Pass Barcode/ Mobile QR code if available

   i. The Travel data is updated to the Digi Yatra ID travel credential now

l. The Digi Yatra ID App then shares the relevant data to the Airport, Airline and Immigration authorities (International (INT) travel)

   i. Consent to share the data is integral part of the app process

m. In case of failure to match the live face with reference face received (as per the step i. above) OR if the passenger is using any other ID not supported for online verification, there will be an activation of Digi Yatra ID Travel Credential with a flag being created and a QR code generated for a one-time physical Identity Document validation by the CISF at the airport registration kiosk.

i. The once in a lifetime validation of the Digi Yatra Travel Credential is done at the airport in order to ensure maximum security.
ii. At the Airport Digi Yatra Registration Kiosk, Passenger scans the Mobile QR Code on the App.
iii. Kiosk Captures passenger's face biometrics
iv. The CISF security staff physically validates the passenger's identity proof
v. The CISF security staff accepts the passenger's registration
vi. The Digi Yatra ID travel credential is now validated, and the passenger's App is updated with the face biometric data
vii. Digi Yatra ID travel credential registration is now fully completed
viii. Digi Yatra ID updated face biometric is sent to the passenger's app for update to the Digi Yatra ID travel credential.

n. Provision shall also be made for the Head of the family to enroll for spouse, minor children, dependent parents or other close relatives, from the same mobile app

i. The enrolment process shall involve scan of the GOI approved ID document of the family member or AADHAAR ID document with validation in case it is possible

STEP 0 (B): DIGI YATRA ID TRAVEL CREDENTIAL: CREATION FROM AIRSEWA, AIRLINE/ OTA TICKET BOOKING SITE/ DY APP/ AIRPORT APP (DRIVING LICENSE)

a. Passenger downloads the AirSewa/Airline/ OTA/ Airport App and installs it on his/ her smartphone. The DY SDK will provide the registration interface to all applications.
b. Passenger starts enrolment process by entering the following/ scan the ID
    i. Name (First, Middle, Last name)
    ii. Mobile number
    iii. Email address
    iv. Driving License number
c. Digi Yatra ID app sends an OTP to the passenger's registered mobile number/ email id
d. Passenger enters the OTP received on the mobile number/ email id
e. Driving license database then sends the driving license data to the passenger on the Digi Yatra ID app
f. **Optional:** Passport first page scan and e-passport reading with passport reference face
g. The Digi Yatra ID app extracts the reference face from the driving license data
h. Passenger is prompted to take a selfie with liveness detection and 3D image capture
i. The live face is matched with the reference face and if successful, the Digi Yatra ID Travel credential is created
j. The Digi Yatra ID Travel credential is stored in the Digi Yatra App (in a secure wallet in the smartphone)
k. Passenger can now update the travel data by uploading the Ticket/ Boarding pass or by Scanning the ETKT/ Boarding Pass Barcode/ Mobile QR code if available
    i. The Travel data is updated to the Digi Yatra ID travel credential now
l. The Digi Yatra ID app then shares the relevant data to the Airport, Airline and Immigration authorities (INT travel)
m. In case of failure to match the live face with reference face received (as per the step i. above) OR if the passenger is using any other ID not supported for online verification, there will be an activation of Digi Yatra ID Travel Credential with a once in lifetime process at the registration kiosk at the Airport.
    i. In order to ensure maximum security, a once in a lifetime validation of the Digi Yatra travel credential is done at the airport.
    ii. At the Airport Digi Yatra Registration Kiosk, passenger scans the Mobile QR Code on the App.
    iii. Kiosk Captures passenger's Face biometrics
    iv. The CISF security staff physically validates the passenger's Identity Card

v. The CISF security staff accepts the passenger’s registration
vi. The Digi Yatra ID travel credential is now validated, and the passenger’s App is updated with the face biometric data
vii. Digi Yatra ID Travel Credential registration is now fully completed
viii. Digi Yatra ID updated face biometric is sent to the passenger’s App for update to the Digi Yatra ID travel credential

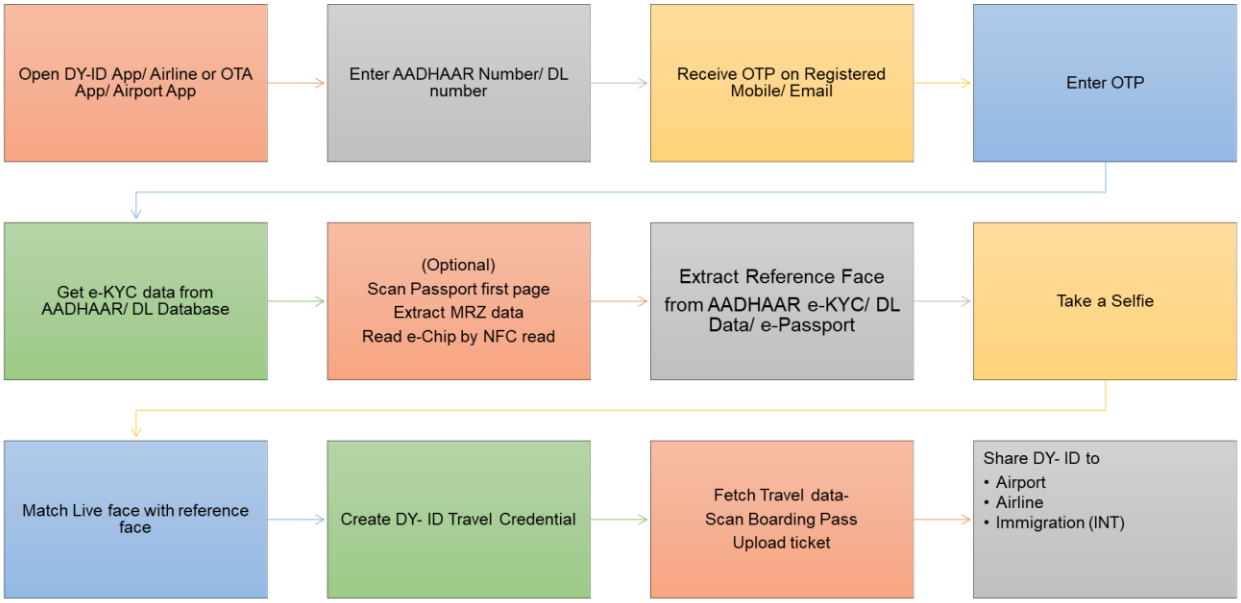
n. Provision shall also be made for the Head of the family to enroll for spouse, minor children, dependent parents or other close relatives, from the same mobile app
   i. The enrolment process shall involve scan of the GOI approved ID document of the family member or AADHAAR ID document with validation in case it is possible

NB: Enrolment using other Govt. of India approved ID databases may be taken up in later phases

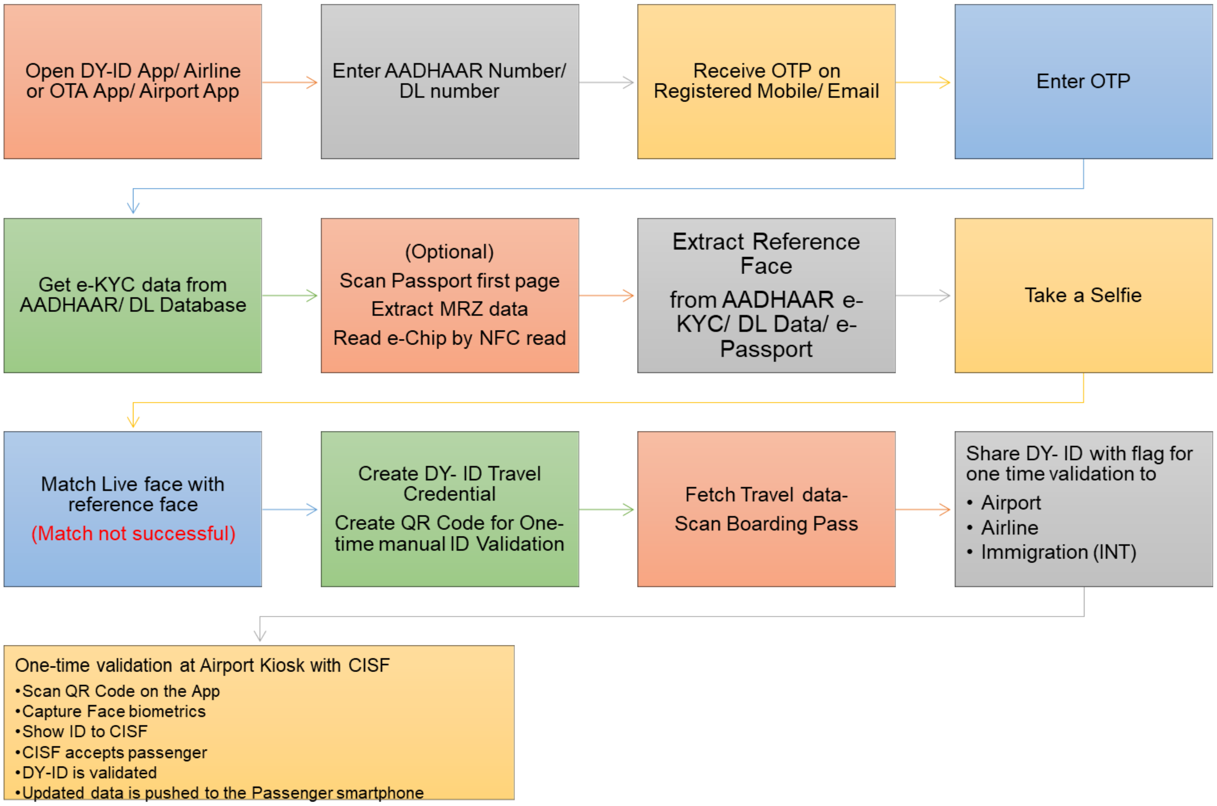
STEP 0 (C): DIGI YATRA DAY OF TRAVEL ONLY: ENROLMENT AT THE AIRPORT ONLY FOR THE DAY OF THE JOURNEY

a. Passenger starts enrolment process at the Registration Kiosk by Scanning the boarding pass barcode/ Mobile QR code
b. The Boarding pass/ E-Ticket with barcode/ Mobile QR code is digitally validated with the airline DCS
c. Kiosk Captures passenger’s Face biometrics
d. The CISF security staff physically validates the passenger’s Identity Card (Any Govt. of India approved ID card)
e. The CISF security staff accepts the passenger’s registration/ enrolment for the day of the journey
f. Passenger is now free to move to the entry e-gates.
g. The enrolment is valid only for the journey and biometric data is purged from the local airport biometric system after the defined period of storage.

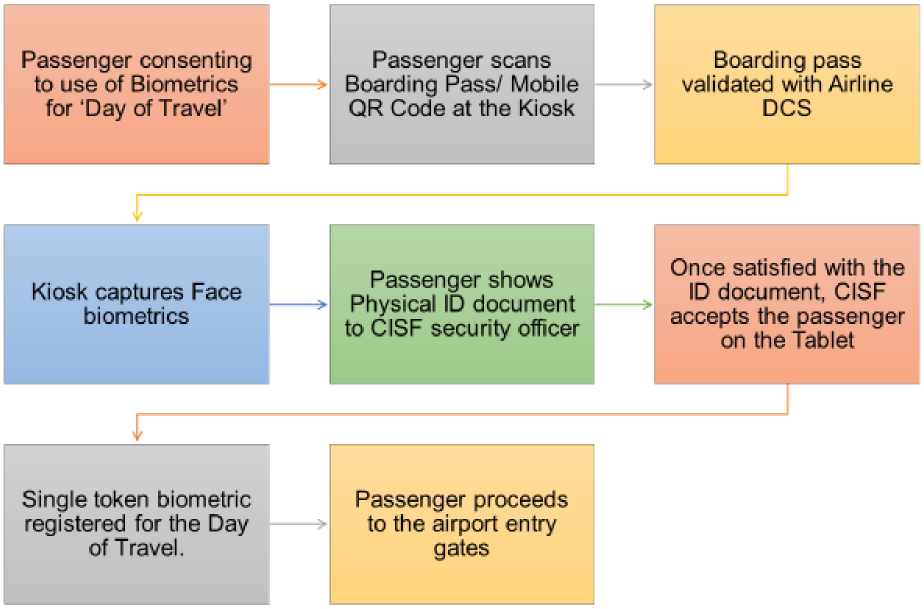
REGISTRATION PROCESS FLOW WITH AADHAAR/ DL IN CASE SELFIE BIOMETRIC MATCHING IS SUCCESSFUL


Open DY-ID App/ Airline or OTA App/ Airport App
Enter AADHAAR Number/ DL number
Receive OTP on Registered Mobile/ Email
Enter OTP
Get e-KYC data from AADHAAR/ DL Database
(Optional)
Scan Passport first page
Extract MRZ data
Read e-Chip by NFC read
Extract Reference Face from AADHAAR e-KYC/ DL Data/ e-Passport
Take a Selfie
Match Live face with reference face
Create DY- ID Travel Credential
Fetch Travel data-
Scan Boarding Pass
Upload ticket
Share DY- ID to
• Airport
• Airline
• Immigration (INT)

REGISTRATION PROCESS FLOW WITH AADHAAR/ DL, IF SELFIE BIOMETRIC MATCHING IS UNSUCCESSFUL


Open DY-ID App/ Airline or OTA App/ Airport App
Enter AADHAAR Number/ DL number
Receive OTP on Registered Mobile/ Email
Enter OTP
Get e-KYC data from AADHAAR/ DL Database
(Optional)
Scan Passport first page
Extract MRZ data
Read e-Chip by NFC read
Extract Reference Face
from AADHAAR e-KYC/ DL Data/ e-Passport
Take a Selfie
Match Live face with reference face
(Match not successful)
Create DY- ID Travel Credential
Create QR Code for One-time manual ID Validation
Fetch Travel data-
Scan Boarding Pass
Share DY- ID with flag for one time validation to
• Airport
• Airline
• Immigration (INT)
One-time validation at Airport Kiosk with CISF
•Scan QR Code on the App
•Capture Face biometrics
•Show ID to CISF
•CISF accepts passenger
•DY-ID is validated
•Updated data is pushed to the Passenger smartphone

REGISTRATION PROCESS FLOW FOR DAY OF TRAVEL REGISTRATION ONLY



Passenger consenting to use of Biometrics for 'Day of Travel'

Passenger scans Boarding Pass/ Mobile QR Code at the Kiosk

Boarding pass validated with Airline DCS

Kiosk captures Face biometrics

Passenger shows Physical ID document to CISF security officer

Once satisfied with the ID document, CISF accepts the passenger on the Tablet

Single token biometric registered for the Day of Travel.

Passenger proceeds to the airport entry gates

DIGI YATRA ID TRAVEL CREDENTIAL- HANDLING OF PERSONAL DATA

a. The Digi Yatra process allows passengers to share the data with various stakeholders Viz. Airlines, Online Travel Agents (OTAs), Airports, Immigration authorities etc.

b. The solution shall be built on the fundamental principles of "Privacy by Design"

c. Passenger has all the data (Travel details, Identity details etc.) in a secure wallet on the Digi Yatra ID App in his/ her smartphone.
   - i. Information is stored as verifiable Digital Travel Credential in the passenger's secure wallet
   - ii. End to end, peer to peer encrypted communication, security standards at par with but not inferior to the requirements as per NIST CSF, ISO 27001, IT ACT 2000, Data Privacy Act (or regulation) and or any other application act / law / regulation which may come in to effect in future

d. Passenger is empowered to control his/her personal data in the following aspects
   - i. To whom the data is shared with.
     - i. Airlines/ OTAs
     - ii. Airports
     - iii. Immigration authorities (for International travel)
   - ii. What data is shared.
     - i. Name
     - ii. ID details (e.g.: AADHAAR, PAN etc.)
     - iii. Single token biometric face
     - iv. Passport data (if & as needed)
   - iii. When it is shared
     - i. Defined time before STD of the flight

e. The face biometrics data is purged out from the Airport Digi Yatra Biometric Boarding System (DYBBS) system 24 hours after the Passenger's flight takes off

These steps are to ensure passenger personal data is protected from unauthorized access, use and/or disclosure

DIGI YATRA VALUE-ADDED SERVICES: CONSENT & OPT IN/ OPT OUT

a. An explicit consent is taken from Passengers who wish to subscribe/ avail of value-added services from the Digi Yatra ecosystem stakeholders/ partners

b. Passengers can "Opt in/ Opt Out" from such services at any given point of time

c. Based on the consent, passengers may share mobile number/ email id with the Airport DYBBS / other ecosystem partners like Hotels, Approved Cab Operators, Participating Hotels, Lounges etc.

   i. **Sample Consent Note:**

I, (*Name of the Passenger)*, hereby willfully consent to use my phone number & email ID, Ticket/ Boarding Pass Data & Face Biometric data, to subscribe, avail value added services from the Digi Yatra ecosystem stakeholders / partners.

RE-CREATION OF DIGI YATRA ID

a. In case if any Passenger changes his/ her smartphone, he/ she can re-create the Digi Yatra ID Travel Credentials as per the original enrolment process
b. In case the Passenger changes the smartphone, there will be a possibility of transferring the DY-ID credentials from one phone to another.
c. This process will be mapped on to the Digi Yatra App, so that there won't be a need for a re-enrolment

GOVT. OF INDIA IDENTITY DOCUMENTS ACCEPTED FOR DIGI YATRA ID TRAVEL CREDENTIAL (AS PER BCAS REGULATIONS AND GUIDELINES)

a. For the Purpose of registering for Digi Yatra ID, the passenger can use Govt. of India issued Photo Identity Cards as follows (Not exhaustive)
   i. AADHAAR ID: Fully self service
   ii. Driving License: Fully self service
   iii. Passport: With manual validation at the airport registration kiosk
   iv. PAN: With manual validation at the airport registration kiosk
   v. Voter ID: With manual validation at the airport registration kiosk
   vi. Student ID: With manual validation at the airport registration kiosk

STEP-1A AIRPORT ENTRY GATE (PASSENGER WITH DIGI YATRA ID TRAVEL CREDENTIAL, SHARED WITH THE AIRPORT OR BIOMETRICS REGISTERED FOR DAY OF TRAVEL)

SINGLE PASSENGER WITH QR CODED TICKET OR BOARDING PASS (BCBP)

a. Passenger comes to the Airport with E-Ticket with Barcode/ QR code and reaches the entry e-Gate at the Airport

OR

b. Passenger comes to the Airport checked-in with a Paper Boarding Pass and/or E-Mobile Boarding Pass with Barcode/ QR code
c. At the Airport entry gates, Passenger scans his/ her Boarding Pass/ ETKT Barcode/ Mobile QR code
    i. The Scan barcode/ Mobile QR code process may not be required, and passenger can be directly identified and verified with the help of only the live face matched with the reference face from the DY-ID travel credential. This will eliminate the need for scanning the BCBP (Barcode/ Mobile QR Code)
    ii. The same will be rolled out in phases, based on the approvals received from BCAS.

d. The E-Gate validates the travel document with the Airline DCS
e. Digi Yatra Biometric Boarding System (DYBBS) E-Gate captures in one single Capture the Passenger’s face biometrics
f. Verifies the live face biometrics with the DY-ID Travel Credential reference face data
g. If biometric face verification is successful, the e-gate opens
h. Passenger can walk through the e-gate into the Airport
i. ‘Passenger Live Dataset’ for the journey is created for further reference at the remaining check points at the airport.
j. Digi Yatra Biometric Boarding System (DYBBS) does three important verifications
    i. E-Ticket/ Boarding Pass validation with the Airline DCS
    ii. Establish Identity of Passenger with real-time Biometric Validation with the Digi Yatra ID Travel Credentials
    iii. Validates Time limits to permit Passenger entry into the Airport
k. “Passenger Dataset” with the (Face Biometric + PNR) is created with a unique identifier as the single token
l. In case of unsuccessful validation, Passenger’s ID is manually checked by the Security Staff and only after CISF Security Accepting the Passenger in the system, the “Passenger Dataset” is created.

AIRPORT ENTRY E-GATES- CISF ROLE

a. The CISF staff will be enrolled/ logging into the Digi Yatra Biometric Boarding System (DYBBS) System.

b. The “Passenger Digi Yatra ID Travel Credential” is used to verify the passenger’s identity

c. CISF security staff does only exception handling & passenger profiling.

d. CISF security staff Intervenes only on the red & amber alerts

e. Display for security will show Passenger details in a green envelope

f. CISF Security Staff at the Airport entry e-gate gets a display of passenger’s face biometrics & travel document (Ticket/Boarding pass) verification status whether successful or not.

    i. In case of validation being unsuccessful, the Passenger is subject to a manual ID check before being permitted/ accepted by the CISF Security Staff

AIRPORT “PASSENGER LIVE DATASET”

a. Digi Yatra Biometric Boarding System (DYBBS shall store the passengers following data and store it as a “Passenger Live Dataset”

    i. Passenger Check in information with the following mandatory fields

        i. PNR

        ii. Passenger Name

        iii. Flight number

        iv. Date & Time of Flight

        v. From & to Destination

        vi. Sequence Number

        vii. Seat Number

    ii. Passenger’s Face Biometrics in the form of a Digital Template

    iii. A unique identifier for each Passenger

B. The “Passenger Live Dataset” shall be used for all further Identification of the Passenger using “Biometrics or Barcode/ Mobile QR Code/ BCBP as a Single Token” at all other Checkpoints until Boarding

STEP-1B AIRPORT ENTRY GATE- NON-BIOMETRIC PROCESS (PASSENGER WITHOUT DIGI YATRA ID TRAVEL CREDENTIAL/ BIOMETRIC REGISTRATION)

SINGLE PASSENGER WITH BARCODE/ QR CODED TICKET OR BOARDING PASS (BCBP)

a. Passenger comes to the Airport with E-Ticket with Barcode/ Mobile QR code and reaches the entry e-Gate at the Airport

OR

b. Passenger comes to the Airport checked-in with a Paper Boarding Pass and/or E-Mobile Boarding Pass with Barcode/ QR code
c. At the Airport entry gates, Passenger scans his/ her Boarding Pass/ ETKT Barcode/ Mobile QR code
d. The E-Gate validates the travel document with the Airline Departure Control System (DCS)
e. The travel document validation is shown to the CISF security officer on a tablet.
f. The passenger then shows the physical ID card to the CISF security officer
g. If the CISF Security officer is satisfied with the ID card, he/ she accepts the passenger on the tablet.
h. Upon acceptance by the CISF security, the E-Gate opens
i. Passenger can walk through the E-Gate into the Airport
j. Passenger must scan the Barcode/ Mobile QR code and a manual ID card check by CISF authorities at relevant checkpoints may be necessary at the other checkpoints inside the airport from the Airport entry to the boarding gates.
k. Digi Yatra Biometric Boarding System (DYBBS) does two important verifications
    i. E-Ticket/ Boarding Pass validation with the Airline DCS
    ii. Validates Time limits to permit Passenger entry into the Airport
l. In case of unsuccessful validation, Passenger’s ID and Ticket are manually checked by the Security Staff and only after CISF Security Accepting the Passenger in the system, the Passenger is permitted into the Airport Terminal.

AIRPORT ENTRY E-GATES- CISF ROLE

a. The CISF staff will be enrolled/ logging into the Digi Yatra Biometric Boarding System (DYBBS) system.
b. The CISF staff checks the passenger ID card physically
c. Display for Security will show Passenger details in a Green Envelope

STEP-2A AIRPORT CHECK-IN KIOSK (2 STEP PROCESS WITH SELF BAG DROP/ HYBRID BAG DROP)

STEP-1 OF THE 2-STEP PROCESS

a. If Passenger has entered the Airport with only E-Ticket,
   i. He/ She moves to the Common Use Self Service (CUSS) Kiosk
   ii. Passenger is identified by his Biometric on the Biometric Reading device (Face)
      i. If passenger has opted for the non-biometric flow the passenger has to scan the Barcode/Mobile QR Code on Boarding Pass.

b. "Passenger Live Dataset" is used to authenticate passenger

c. The Digi Yatra Biometric Boarding System (DYBBS) system is able to identify the Passenger Flight from the 'Passenger Live Dataset, validated with the PNL and automatically opens the Check-in app/ function of the relevant Airline in the Kiosk.

d. Once this validation is completed, the Passenger has to make a choice of the seat/ Frequent Flyer number etc.

e. Passenger does his seat selections and Checks-in
   OR

f. If Passenger has already Checked in and has a Mobile Boarding Pass or Home Printed Boarding Pass
   i. Passenger moves to the CUSS Kiosk
   ii. Passenger is identified by his biometric on the Biometric Reading device (Face)
      i. If passenger has opted for the non-biometric flow the passenger has to scan the Barcode/Mobile QR Code on Boarding Pass.

g. Passenger Selects the number of baggage tags to be printed

h. Prints & collects the baggage Tags.

i. The system updates the status of check-in on the "Passenger Live Dataset" for use at further Check Points

j. Passenger then tags his bag and moves towards the Self Baggage Drop Area

STEP-2B BAGGAGE DROP (2 STEP PROCESS WITH SELF BAG DROP/ HYBRID BAG DROP)

STEP-2 OF THE 2-STEP PROCESS

a. Passenger walks towards the Baggage Drop unit/ Counter, he/ she is identified by his/ her Biometric on the Biometric Reading device (Face)

        i. If passenger has opted for the non-biometric flow the passenger has to scan the Barcode/QR Code on Boarding Pass.

b. "Passenger Live Dataset" is used to authenticate the passenger & flight details shown on the display
c. Passenger is prompted to deposit the bags in the Self Bag Drop Machine.
    i. This process could also be used with a manually assisted bag drop service.
d. Passenger is issued with a baggage claim slip as an acknowledgement of the received bag.
e. Baggage tags are linked to the unique identifier of the traveler

STEP-3 PESC ENTRY CHECK TO THE SHA

a. Entry check to the SHA is done at the PESC Zone. Entry is restricted to registered and authenticated passengers only.
b. Passenger is identified by his/ her Face Biometrics or Barcode/QR Code on Boarding Pass at the E-Gate Biometric/ Barcode/ QR reader, using the "Passenger Live Dataset"
    i. Passengers using the non-biometric flow shall scan the Barcode/ QR Code on Boarding Pass
        i. There is no manual intervention by CISF
c. The E-Gate Opens
d. Passenger then enters the PESC Zone

STEP-4 PESC FRISKING

a. Entry to the PESC is regulated & controlled using biometric validation with the "Passenger Live Dataset"
b. Therefore, there is no further need to validate the passenger or stamp the boarding pass by the CISF Staff as is the current practice.
c. Passenger divests his personal belongings into the X-Ray Machine / CT-Scan Machine (Smart Lane Enhanced Hand Baggage Screening System with Automated Tray Return)
d. Passenger then moves through the DFMD/ Body Scanner (If Installed)
    i. In case of Door Frame Metal Detector (DFMD) CISF Officer carries out the frisking of the passenger and clears him/her after verifying/ satisfying himself, clears the passenger.
    ii. If he/ she is clear of any threat items, then he/ she moves to the X-Ray output lanes to collect his belongings from the tray

e. If any additional checks are needed the Passenger is subjected to the same as per the SOP of the CISF
f. Cameras in the PESC Area shall be used to monitor the proceedings in the Frisking Area & can be used for any Forensic Analysis

OPTIONAL ADDITIONS TO THE PESC PROCESS

Based on specific requirements of any airport, additional non-intrusive data capturing elements such as camera, sensors etc. may be added to the system to capture Passenger Queue-waiting times, Queue Lengths & processing times. However, the Passenger related process shall remain unchanged as mentioned in this policy document.

STEP-5 BOARDING GATE

a. Passenger is identified using the "Passenger Live Dataset" using his/ her Face Biometrics
    a. Passengers using the non-biometric flow shall scan the Barcode/ Mobile QR Code on Boarding Pass at the E-Gate Biometric/ Barcode/ Mobile QR Code reader
        i. There is no manual ID verification by the airline staff
b. Passenger then enters the boarding gate
c. The Airline DCS is updated for passenger boarding status
d. Airline staff gets to see the status of boarding on a real-time dashboard

STEP-6 AIRCRAFT

a. Passenger proceeds to board the Aircraft
b. Passengers shall be validated digitally by the Airlines (if needed).
c. At a future date, it is proposed to have a face recognition reader for this purpose. This could be on a smartphone/ Tablet with Face recognition using the Digi Yatra Biometric Boarding System (DYBBS) "Passenger Dataset" to display passenger flight details and seat number

EXCEPTIONS PROCESSES:

FLIGHT RESCHEDULING/ REBOOKING OF TICKET

a. If any Passenger enters the Airport on a valid ticket & subsequently finds that
    i. The flight is cancelled or
    ii. If he/ she intends to change the flight

iii. He/ She can go to the Airline ticketing counter and reschedule his/ her ticket to another flight

b. A standard operating process is followed where the rescheduling and update to the Passenger Data Set happens at a registration kiosk in the check-in hall

c. Changes in Flight/ Airline is updated on the Digi Yatra Biometric Boarding System (DYBBS)

d. If Passenger cancels his/ her ticket & travel plans then,

   i. The travel cancellation is recorded

   ii. Passenger is authenticated using his/ her biometrics & escorted by the Airline Staff, validated by the CISF Supervisor and records are updated.

      a. For non-biometric flow passengers, a scan of the ETKT/ Boarding Pass Barcode/ Mobile QR Code and a manual ID check is done

   iii. He/she will be escorted by the concerned airline staff to the CISF and after making log entry by the CISF at the Security Hold Area and subsequently at the departure entry point

   iv. The said Passenger would be allowed to exit the terminal building

   v. Passenger the exits the Airport Building

DE-BOARDING/ OFFLOADING AND EXIT/ RE-ENTRY TO FROM A PARTICULAR ZONE

a. If any Passenger enters the Airport on a valid ticket & subsequently finds that

   i. He/ She has to move back for some unforeseen reasons

   ii. He/ She can go to the previous process stage under escort of the Airline staff and later comeback to the same process checkpoint to proceed further towards the boarding gate

b. A standard operating process is followed where the rescheduling and update to the Passenger Data Set happens at a Registration Kiosk in the check-in hall/ any other area.

c. Changes in Flight/ Airline is updated on the Digi Yatra Biometric Boarding System (DYBBS)

d. If Passenger cancels his/ her ticket & travel plans then,

   i. The Travel cancellation is recorded

   ii. Passenger is authenticated using his/ her biometrics & escorted by the Airline Staff, validated by the CISF Supervisor and records are updated.

      a. For non-biometric flow passengers, a scan of the ETKT/ Boarding Pass Barcode/ Mobile QR Code and a manual ID check is done

iii. He/she will be escorted by the concerned airline staff to the CISF and after making a digital log entry by the CISF at the Security Hold Area SHA/ any other area and subsequently at the departure entry point

iv. The said passenger would then be allowed to exit the terminal building

v. Passenger then exits the Airport building

TRANSFER PASSENGER PROCESS

a. Transfer Passenger shall have shared the Digi Yatra ID travel Credentials to the transit airport and can follow the same biometric process. If Digi Yatra ID travel credential is not shared, passenger may be allowed to go through the transfer area by
   i. Scanning the boarding pass at the designated Kiosk/ e-gate
   ii. Sharing the Digi Yatra ID travel credentials if not already shared or showing any other Govt. ID proof to the CISF Security Staff and/ or use passport document for domestic to international transfer passengers
   iii. Registering the passenger’s face biometrics may be made available at the transfer area
   iv. “Passenger Live Dataset” is updated to his/her specific flight

DOMESTIC ARRIVALS: STANDARD OPERATING PROCESS

STEP-1: ARRIVING INTO THE AIRPORT

a. Passengers enter the Airport building
b. Collects his baggage from the baggage claim belt
c. Exits the Airport building

INTERNATIONAL DEPARTURES- STANDARD OPERATING PROCESS

STEP-1: TICKET BOOKING

a. Ticket Booking: On the Airline Reservation System, Portal or App & On other Agencies Viz. Online Travel Agents (OTA)/ Global Distribution Systems (GDS)
    i. While booking a ticket the same process of Digi Yatra ID Travel Credential sharing is followed as explained in STEP 0-A/ O-B

b. Airlines and Online Ticketing Agencies shall issue a Ticket with a Barcode/ Mobile QR code as per **IATA Resolution 792** which has the following minimum data:
    i. PNR number
    ii. Passenger Name (Last name & First name)
    iii. Flight number
    iv. From and To Destinations
    v. Date of Flight
    vi. Time of Departure
    vii. Foreign/ Indian Citizens Passport number in the Passport Field (Need based)

STEP-2 HOME CHECK-IN/ WEB CHECK-IN

a. On the Airline App/ Website, the passenger completes the seat selection & checks-in to the flight

b. Passenger gets his/ her boarding pass printed at home or gets an e-Mobile boarding pass

   i. Passengers shall have the option of check-in using web check-in/ mobile check-in, before reaching the Airport to facilitate the process of identification of passenger and easy validation of the bona-fides of the Passenger’s Ticket.

   ii. Bar coded boarding pass shall be as per IATA Resolution 792

c. Passengers may also come to the Airport with just their ETKT with Barcode/ QR code (ETKT with Barcode/ QR code as per IATA Resolution 792)

STEP-3 AIRPORT ENTRY GATE: E-GATE

SINGLE PASSENGERS WITH INDIAN & FOREIGN PASSPORTS

a. Passenger goes straight to the departure entry E-Gate

b. Scans passport first page

c. Validation of Passport (IR/ UV/ features) & Airline DCS done

   i. For India Passport holders, the passport number with passenger name is validated with the Passport Database

   ii. For international passengers the image from an electronic passport chip is retrieved using public shared key & face matching is done

d. On Successful validation, Passenger’s facial biometrics are captured, and Passenger is guided by visuals/ (if possible, audio) by the Digi Yatra Biometric Boarding System (DYBBS) Software on the Kiosk/ E-Gate to co-operate in the process of capture. (Passenger Face+Iris can be captured simultaeneously as an option.)

e. Digi Yatra Biometric Boarding System (DYBBS) does four important verifications

   i. Document check for authenticity, UV/ IR Checks & also passport features check

   ii. Validation of Passport Document for genuineness and validation with passport database

      i. For international passengers the image from an electronic passport chip is retrieved using public shared key & face matching is done

   iii. Passenger Ticket/ BCBP/ Mobile Boarding Pass Mobile QR code is validated with the Airline DCS using the Passport data

   iv. Passenger Name matching on E- Ticket/ Boarding Pass with Name on Passport

   v. Validates Time limits to permit entry into the Airport

f. Passenger thus registers his Biometrics (Face) for identification at other checkpoints
g. In case of unsuccessful validation, Passenger's passport is manually checked by the security staff and passenger is accepted upon satisfactory manual passport check.
h. Once Validation is Successful, "Passenger Dataset" with Single Biometric Token of Face is created, with a unique identifier.

NB: Optionally additional step with registration kiosks may be added for carrying out similar functions

AIRPORT ENTRY GATE- CISF ROLE

a. The CISF staff will be enrolled into the System with their Face Biometrics and every login will be using the Face Biometric
b. The (Passport + Face Biometric + PNR) form the "Passenger Dataset" which is used to authenticate Passenger at every subsequent process Step
c. E-Gates open automatically on positive identification/ validation
d. Display for security will show passenger details in a green envelope
e. CISF security officer does exception handling & passenger profiling
f. CISF security officer intervenes only on the red & amber alerts
g. CISF security officer at the Airport entry gate gets a display of passenger's passport & travel document (ticket/boarding pass) verification status whether successful or unsuccessful
    i. In case of Passport validation/ document check being unsuccessful passenger to be subject to a manual passport check before being permitted by the CISF staff into the Airport building
h. Automated E-Gate will open if passenger is successfully validated manually by the CISF

AIRPORT ENTRY GATE "PASSENGER LIVE DATASET"

a. Digi Yatra Biometric Boarding System (DYBBS) shall store the Passengers following Data and store it as a "Passenger Live Dataset"

    i. Passenger Check in information with the following mandatory fields

        i. PNR
        ii. Passenger Name
        iii. Flight number
        iv. Date & Time of Flight
        v. From & to Destination

vi. Sequence Number

vii. Seat Number

viii. Passport Number

ii. Passenger’s Face Biometrics

iii. A unique identifier for each Passenger

b. The “Passenger Live Dataset” shall be used for all further Identification of the Passenger using “Biometrics as a Single Token” at all other checkpoints until Boarding.

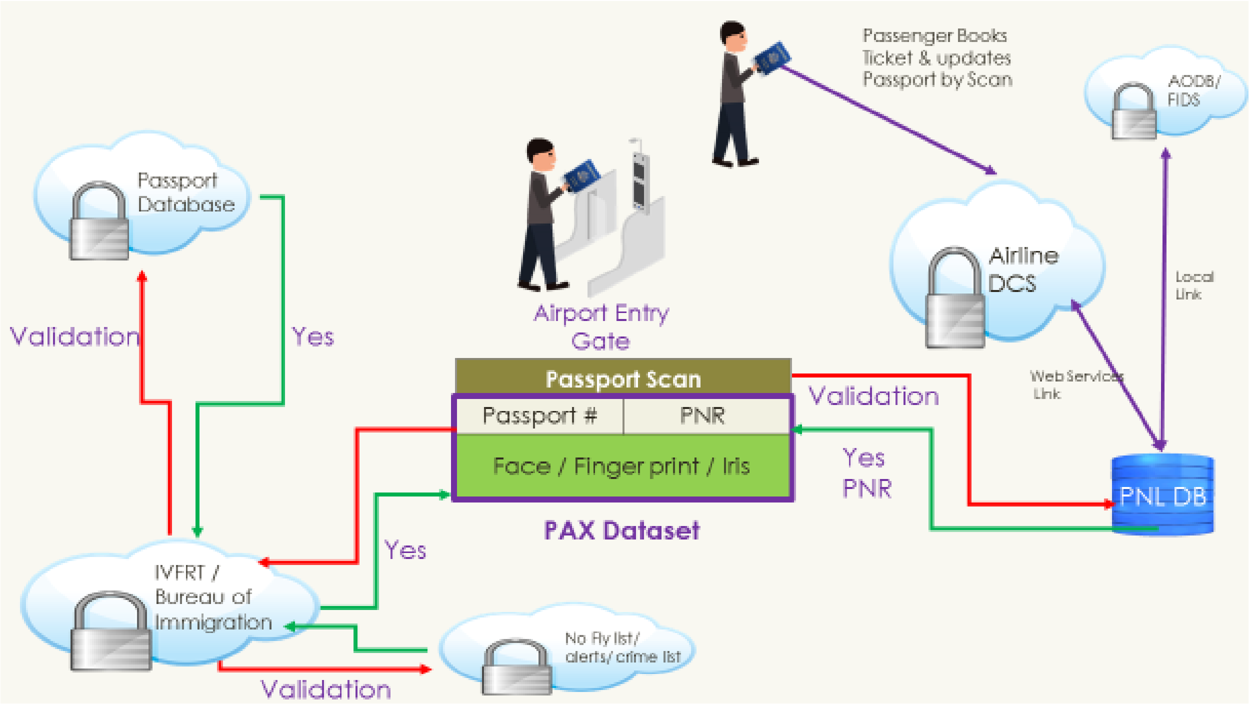
c. On successful authentication, a green signal is given to the passenger to proceed to the Airport entry E-Gate.

d. Passenger then moves towards the E-Gate at the Airport entry & presents his/ her Face Biometric on the Face Biometric Reading device.

e. Upon Successful Authentication with the “Passenger Live Dataset” The E-Gate Opens, Passenger enters the Airport.

NB: Digi Yatra Biometric Boarding System (DYBBS) shall provide real time Passengers’ data to the Immigrations

OPERATING PROCESS - CONCEPT ONLY



GROUP PASSENGERS WITH BARCODE/ QR CODED TICKET / BOARDING PASS (BCBP) EACH PASSENGER HAS AN INDIVIDUAL TICKET / BOARDING PASS (BCBP)

a. Families with Infants (below 2 years)

b. Groups with all Adults and Minors

c. Separate Lanes with CISF Security Officer intervention for all the Group Passengers

d. Passenger from the Group Scans the first page of the Passport on the Registration Kiosk/ E-Gate

e. Passenger Ticket is validated with the Airline DCS using the Passport data

f. On Successful validation, Passenger's Facial Biometrics are captured

g. Biometric E-Boarding Processing System (DYBBS) does four important verifications

   i. E-Ticket/ Boarding Pass validation with the Airline DCS
   ii. Validation of Passport Document for genuineness and validation with Passport Database

iii. Passenger name matching on E- Ticket/ Boarding Pass with name on Passport
iv. For International passengers the image from an electronic passport chip is retrieved using Public Shared Key (for all those countries who allow the reading of the e-chip) & Face matching is done
v. Validates time limits to permit entry into the Airport

h. Passenger thus registers his Biometrics (Face) for identification at other checkpoints

i. In case of unsuccessful validation, passenger's passport is manually checked by the security staff and passenger is accepted upon satisfactory manual passport check.

j. "Passenger Dataset" is created with unique identifier as single token

k. Similarly, for all other adult passengers the same process as per clause above (d), (e) & (f) are followed.

l. If the passenger is an infant (below 2 years) then the infant will be tagged to the head of the group and for all process points by default, the infant will be tagged to the passenger as per choice made by the passenger in the group/family

STEP-4A AIRPORT CHECK-IN (2 STEP PROCESS WITH SELF BAG DROP/ HYBRID BAG DROP)

STEP-1 OF THE 2-STEP PROCESS

a. If Passenger registers and enters the Airport with only E-Ticket,
   i. Passenger moves to the CUSS Kiosk
   ii. Passenger is recognized by the Face Biometric by the biometric reading device
      i. For non-biometric flow passengers, a passport scan and/ or boarding pass scan may be needed
b. "Passenger Live Dataset" is used to authenticate passenger
c. The Digi Yatra Biometric Boarding System (DYBBS) system is able to identify the passenger flight from the 'Passenger Live Dataset', validated with the PNL and automatically opens the check-in app/ function of the relevant Airline in the kiosk.
d. Once validated, the passenger makes his choice of seat/ Frequent Flyer number etc.
e. Passenger does his seat selections and checks-in

OR

f. If passenger has already checked in and has a Mobile Boarding Pass or Home Printed Boarding Pass
    i. Passenger moves to the CUSS Kiosk
    ii. Passenger is identified by the Face Biometric by the biometric reading device
        i. For non-biometric flow passengers, a passport scan and/ or boarding pass scan may be needed

g. Passenger selects the number of baggage tags to be printed
h. Prints & collects the baggage Tags.
i. The system updates the status of Check-in on the "Passenger Live Dataset" for use at further check points
j. Passenger then tags his bag and moves towards the Self Baggage Drop Area

STEP-4B BAGGAGE DROP (2 STEP PROCESS WITH SELF BAG DROP/ HYBRID BAG DROP)

STEP-2 OF THE 2-STEP PROCESS

a. Passenger is identified by the Face Biometric by the biometric reader
b. "Passenger Live Dataset" is used to authenticate the passenger & flight details shown on the display
    i. For non-biometric flow passengers, a passport scan and/ or boarding pass scan may be needed

c. Passenger then deposits the bags in the Self Bag Drop Machine.
    i. This process could also be used with a manually assisted bag drop service.

d. Passenger is issued with a baggage claim slip as an acknowledgement of the received bag.
e. Bag tags are linked to the unique identifier of the traveler

STEP-5 TRANSFER Passenger PROCESS

a. Transfer Passenger shall have to register to the Digi Yatra Biometric Boarding System (DYBBS) authentication system
b. Passenger scans the first page of the passport on the registration kiosk/ E-Gate
c. Passenger Ticket is validated with the Airline DCS using the passport data
d. On Successful validation, passenger's facial biometrics are captured

    i. For non-biometric flow passengers, a passport scan and/ or boarding pass scan may be needed

e. Digi Yatra Biometric Boarding System (DYBBS) does four important verifications
    i. Document check for authenticity, UV/ IR Checks & also passport features check
    ii. Passenger Ticket/ BCBP is validated with the Airline DCS using the passport data
    iii. For Domestic passengers, using the connectivity to the Passport Seva Project (PSP) database a face matching is done with the passengers' captured face.
    iv. For International passengers the image from an electronic passport chip is retrieved using public shared key & face matching is done
f. "Passenger Live Dataset" is created/ updated to his/her specific flight

NB: For Passengers who are on Domestic- International and International-International Flights there will be a similar SOP to register the Passenger and to re-validate into the Digi Yatra Biometric Boarding System (DYBBS)

STEP-5 DEPARTURE IMMIGRATIONS (INDIAN & FOREIGN PASSPORT HOLDERS)

a. The immigrations process is carried out through a double flap door/ trap door E-Gate system.
b. Entry to the immigration zone is restricted only to passengers who are registered & authenticated by the Digi Yatra Biometric Boarding System (DYBBS)
c. Passenger is identified using the face biometric in the "Passenger Live Dataset" at the first flap door E-Gate Biometric reader.
d. The first flap door of the dual door E-Gate opens on positive identification with the Digi Yatra Biometric Boarding System (DYBBS) single token of face.
e. Passenger then enters the dual door E-Gate and reaches the second flap door for the immigration clearance.
    i. The first flap door closes once passenger enters the dual gate door to prevent any other passenger from entering inadvertently
f. At the second flap door, passenger scans his/ her passport first page and he/ she is validated with the immigrations database
g. Passenger then presents his biometrics (finger/ face/ iris) as per immigration biometric check process. (The IVFRT Database is updated with the current transaction and face + iris may be updated to the passenger records)

    i. For foreign passengers with E-Passports, an additional check of Face matching with the face retrieved from the passport and actual face captured by the face + iris camera is done. IVFRT records are updated accordingly
    ii. If as per the IVFRT the passenger needs FRRO registration, then passenger is diverted to manual processing immigration counters

h. Once the passenger is validated by the immigration system, the second flap door opens
    i. In case of a reject by the immigrations, the first flap door opens and the passenger is then goes back and is processed through the manual entry counter

i. Successfully validated passenger then moves to the security check zone

NB: Immigrations System is a completely isolated system not connected to the Digi Yatra Biometric Boarding System (DYBBS)

The E-Gate second flap door sends a "Clear" or "Reject" signal of a passenger to the Digi Yatra Biometric Boarding System (DYBBS) , using the E-Gate signals and other sensors in the E-Gate. This ensures that there is complete isolation of the immigration system with the Digi Yatra Biometric Boarding System (DYBBS)
In case of rejection of the passenger at the second flap door, the passenger is asked to go out of the E-Gate and go to the manual counters. In this case the immigrations Central Processing Unit (CPU) sends signal to the first flap door to open.

Visa Checks shall only be done by the Airlines and is considered as an Airline responsibility

STEP-6 PESC HAND BAGGAGE SCREENING AREA & FRISKING

a. The entry to the PESC area is already regulated & controlled and done using face biometric validation with the "Passenger Live Dataset" at the Immigrations area.
b. Therefore, there is no further need to validate the passenger by the CISF Security Staff
c. Passenger divests his personal belongings into the X-Ray Machine / CT Scan Machine (Smart Lane Enhanced Hand Baggage Screening System with Automated Tray Return) (If Installed)
d. Passenger then moves through the DFMD/ Body Scanner

    i. In case of DFMD CISF security officer carries out the frisking of the passenger and clears him/her after verifying/ satisfying himself, clears the passenger
    ii. If he/ she is clear of any threat items, then he/ she moves to the X-Ray output lanes to collect his belongings from the tray

e. If any additional checks are needed the passenger is subjected to the same as per the SOP of the CISF
f. Cameras in the PESC area shall be used to monitor the proceedings in the frisking area & can be used for any forensic analysis

STEP-7 BOARDING GATE

a. Passenger is identified using his/ her face biometrics at the E-Gate Biometric reader
    i. For non-biometric flow passengers, a passport scan and/ or boarding pass scan may be needed as per current process
b. Passenger is identified using the "Passenger Live Dataset"
c. Passenger then enters the boarding area
d. The Airline DCS is updated for passenger boarding status
e. Airline staff gets to see the status of boarding on a real-time dashboard

STEP-8 AIRCRAFT

a. Passenger proceeds to board the Aircraft
b. Passengers shall be validated digitally by the Airlines (if needed)
c. At a future date, it is proposed to have a face recognition reader for this purpose. This could be on a smartphone/ tablet with ace recognition to display passenger flight details and seat number

EXCEPTIONS PROCESSES:

FLIGHT RESCHEDULING/ REBOOKING OF TICKET

e. If Any Passenger enters the Airport on a valid ticket & subsequently finds that
    i. The Flight is cancelled or
    ii. If he/ she intends to change the flight
    iii. He/ She can go to the Airline ticketing counter and reschedule his/ her ticket to another flight

f. A Standard Operating Process is followed where the rescheduling and update to the Passenger Data Set happens at a registration kiosk in the check-in hall

g. Changes in Flight/ Airline is updated on the Digi Yatra Biometric Boarding System (DYBBS)

h. If Passenger cancels his/ her ticket & travel plans then,

   i. The Travel cancellation is recorded

   ii. Passenger is authenticated using his biometrics & taken by the Airline Staff to the CISF Supervisor for updating records

      a. For non-biometric flow passengers, a scan of the ETKT/ Boarding Pass Barcode/ Mobile QR Code and a manual ID check is done

   iii. He/she will be escorted by the concerned airline staff to the CISF and after making log entry by the CISF at the SHA and subsequently at the departure entry point

   iv. The said passenger would be allowed to exit the terminal building

   v. Passenger then exits the Airport Building

DE-BOARDING/ OFFLOADING AND EXIT/ RE-ENTRY TO FROM A PARTICULAR ZONE

e. If Any Passenger enters the Airport on a valid ticket & subsequently finds that

   i. He/ She has to move back for some unforeseen reasons

   ii. He/ She can go to the previous process stage under escort of the Airline staff and later comeback to the same process checkpoint to proceed further towards the boarding gate

f. A Standard Operating Process is followed where the rescheduling and update to the Passenger Data Set happens at a registration kiosk in the check-in hall/ any other area.

g. Changes in Flight/ Airline is updated on the Digi Yatra Biometric Boarding System (DYBBS)

h. If Passenger cancels his/ her ticket & travel plans then,

   i. The Travel cancellation is recorded

   ii. Passenger is authenticated using his/ her biometrics & taken by the Airline Staff to the CISF Supervisor for updating records

      a. For non-biometric flow passengers, a scan of the ETKT/ Boarding Pass Barcode/ Mobile QR Code and a manual ID check is done

   iii. He/she will be escorted by the concerned airline staff to the CISF and after making a Digital log entry by the CISF at the SHA/ any other area and subsequently at the departure entry point

   iv. The said Passenger would then be allowed to exit the terminal building

v. Passenger then exits the Airport Building

TRANSFER PASSENGER PROCESS

b. Transfer Passenger shall have shared the Digi Yatra ID travel credentials to the transit airport and can follow the same biometric process. If Digi Yatra ID Travel Credential is not shared, passenger may be allowed to go through the transfer area by
   i. Scanning the Boarding Pass at the designated kiosk/ e-gate
   ii. Sharing the Digi Yatra ID travel credentials if not already shared or showing any other Govt. ID proof to the CISF Security Staff and/ or use passport document for domestic to international transfer passengers
   iii. Registering the passenger’s face biometrics may be made available at the transfer area
   iv. “Passenger Live Dataset” is updated to his/her specific flight

INTERNATIONAL ARRIVALS: STANDARD OPERATING PROCESS

STEP-1: ARRIVAL INTO THE AIRPORT

a. Passenger enters the Airport building
b. Passenger moves towards the immigration area

STEP-2: ARRIVAL IMMIGRATIONS (INDIAN & FOREIGN PASSPORT HOLDERS)

a. The Arrival Immigrations will consist of Automated Border Control E-Gates with dual flap doors E-Gate
b. At the first flap door of the E-Gate, passenger is allowed to enter as soon as he moves towards the e-Gate and if there is no other passenger in the E-Gate.
c. Once passenger enters the E-Gate, the first flap door closes behind him/ her
d. Passenger then scans his/ her passport first page on the document reader at the second flap door.
e. Airline DCS validation for the passenger is conducted
f. Immigrations system does the following:
    i. Document check for authenticity, UV/ IR Checks & also passport features check
    ii. Passenger Ticket/ BCBP is validated with the Airline DCS using the Passport data
        i. It is understood that there is an existing connectivity from the immigrations system to the Airline DCS, inbound APIs data is available for all flights
    iii. For Indian passengers, using the connectivity to the IVFRT database a face matching is done with the passengers' captured face.
    iv. IVFRT records are updated accordingly with the latest face/ Iris captured at the E-Gate
    v. For Foreign passengers the image from an electronic passport chip is retrieved using public shared key & face matching is done. IVFRT records are updated accordingly with the latest face/ Iris captured at the E-Gate
g. Passengers' Face + Iris biometrics are captured for updating the IVFRT database
    i. For foreign passengers with E-Passports, an additional check of face matching with the face retrieved from the passport and actual face captured by the face + iris Camera is done.
    ii. IVFRT records are updated accordingly with the latest face/ iris captured at the E-Gate

iii. If as per the IVFRT the passenger needs FRRO registration, then E-Gate does not open and the passenger is diverted to manual processing Immigration Counters

h. On successful validation and updating of the transaction, the second flap door of the E-Gate Opens
i. Passenger moves to the customs area/ baggage claim area.

NB: Immigrations system is a completely isolated system not connected to the Digi Yatra Biometric Boarding System (DYBBS).

STEP-3: CUSTOMS PROCESS

a. All passengers move through the green or the red channel without any further process
b. Only if any Passenger is found or caught with contraband goods, the customs officer shall scan passenger's passport and capture face and biometrics of the passenger to update the record into the centralized database maintained by Govt. of India.

STEP-4: EXIT FROM THE AIRPORT

c. Passenger collects his baggage from the baggage claim belt and moves to duty free area.
d. Passenger then walks through the customs red/ green channel and exits the Airport

HIGH LEVEL DATA PRIVACY GUIDELINES

DATA PRIVACY

Airports using the DYBBS shall conform and adhere to the Data Protection laws as applicable and mandated by the GOI.

The DYBBS Data management shall be compliant with IT Act 2000, IT Amendment Act 2008 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 & AADHAR Act 2016 for all the AADHAAR related transactions.

The DYBBS shall also be compliant with other adopted security & privacy requirements as summarized below.

Define & establish a privacy framework which comprises of:

a. A common privacy terminology
b. Define and explain data privacy processing principles as applicable to persons & organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating personal data
c. Define personal data, the actors and their roles in processing personal data
d. Describes controls, measures & considerations for safeguarding personal data

For the Digi Yatra Ecosystem, Periodic Audits, Assessments (by independent teams to assess the level of security and system resilience to protect PII) and Audits (by governing/regulatory bodies e.g. CERT-IN and/or STQC etc., twice every year

a) One privacy impact assessment (e.g. with reference to ISO 27701, GDPR, India PDPA etc.)
b) One security assessment (e.g. ISO 27001) Once every two years shall be conducted by CERT-IN And/ Or STQC or any other Govt. of India nominated agency as applicable

Following are the data privacy processing principles

1. Management & Governance
    a. Define, document, communicate & assign accountability for the privacy policies & procedures
2. Privacy Notice
    a. Give notice in relation to personal data collected, used or disclosed as applicable by the national laws and policies
3. Choice & Consent

    a. Describe clearly the choices available to and obtain implicit / explicit consent in relation to personal data prior to collection & processing

4. Data Minimization
    a. Identify and adhere to the identified purpose for personal information collected
5. Data Inventory & Classification
    a. Define and maintain a data map and inventory, identifying elements by type, sensitivity, retention (need & duration) and storage location

6. Data Protection and Security
    a. Maintain an information security & data protection program that,

        i. Manages risk of data compromise by implementing controls to isolate, detect, and protect personal data
        ii. Manages risk to individuals that may result from the collection, use, retention, in-accuracy, or integrity of personal data, and
        iii. Manages the regulatory non-compliance due to lack of appropriate notice or transparency

7. Third-Party Risk
    a. Maintain a vendor risk management program that assesses vendors on security and privacy practices
8. Data Protection Impact Assessment (DPIA)
    a. Conduct data protection impact assessment to identify, evaluate and mitigate risks to individuals arising as a result of processing their personal data when
        i. the related & relevant programs, systems & processes undergo a change
        ii. a new program, system or process introduced
        iii. a highly sensitive data is processed (e.g. biometric data) or processing any personal data likely to result high risk to the rights & freedom of individual
9. Privacy Incident & Data Breach Management Plan
    a. Implement an incident handling capability for privacy incidents and insider threats that includes preparation, detection and analysis, containment, eradication, and recovery to provide appropriate and timely responses along with establishing a data breach notification plan
    b. Maintain and regularly test the privacy incident & data bream management plan and affected parties
10. Limit use, disclosure & retention
11. Collect, use and retain personal data only for specific, explicit and legitimate purposes accuracy/ quality

    a. Maintain confidentiality, availability and integrity of the personal data

12. Training, Awareness, and Culture
    a. Deploy role-based data privacy training and awareness campaigns
13. Openness/ Disclosure to third parties
    a. Disclosure & sharing of personal data shall be only for the legitimate purposes
14. Challenging Compliance/ Monitoring & Enforcement
    a. Monitor, Report & Track compliance to applicable organizational & regulatory privacy policies, procedures and guidelines. Establish procedures to facilitate disputes, grievances and complaints
15. Data Disposal
    a. This ensures that all data are securely retained, destroyed, anonymized (de-identify) at the end of the process as per the applicable timelines

DATA PRIVACY BY DESIGN PRINCIPLES

Adopt and customize Data Privacy by Design (DPbD) principles such as data minimization, access control etc., in order to protect personal data. Incorporate DPbD principles in business operations, in systems (IT) and product / system / software development lifecycles.

Privacy by Design Principles:

1. Proactive not Reactive; Preventative not Remedial:
    - Anticipate, identify, and prevent invasive events before they happen; which means acting before and not afterward.
2. Privacy as the default setting:
    - Ensuring personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.
3. Privacy Embedded into Design:
    - Privacy measures should not be add-ons, but fully integrated components of the system.
4. Full Functionality – Positive-Sum, not Zero-Sum:
    - Privacy by Design employs a “win-win” approach to all legitimate system design goals; that is, both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both
5. End-to-End Security:
    - Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed.

6. Visibility and Transparency:
    - Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification.
7. Respect for User Privacy:
    - Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

PERSONAL DATA GUIDELINES

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for the specified lawful purpose and shall not be further processed in any manner other than for that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for a longer time than necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the national law.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful access and or processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred nor stored to a country or territory outside India unless it is needed for the purpose of carrying out the passenger Identification/ validation process at the Destination Airport and only with the willful consent from the passenger. “For International Travel, the Biometrics capture (Face, Iris, Fingerprints) process will be as mandated by the Govt. of India as per existing protocols prevalent at that time”
9. Biometric data shall be purged from the Digi Yatra Biometric Boarding System (DYBBS) System 24 hours after the passenger’s journey at the Airport i.e. after completion of boarding and departure of the passengers’ flight.
    a. Digi Yatra Biometric Boarding System (DYBBS) shall have an ability to change the data purge settings based on security requirements on a need basis.
10. Passenger Travel Logs without the biometric data shall be stored for the purpose of audits as per the mandate from Govt. of India. Privacy principles to be applied while deciding what ‘logs’ be stored for audit purpose.
11. Any Security Agency, GOI or other Govt. Agency may be given access to the passenger data based on the current/ existing protocols prevalent at that time.

12. The Digi Yatra Biometric Boarding System (DYBBS) shall be audited as per the requirements of the data protection standards as applicable and mandated by Government of India (GOI).

AADHAAR RELATED PRIVACY GUIDELINES FOR ALL STAKEHOLDERS

AUTHENTICATION OF PASSENGER TO THE AADHAAR DATABASE

a. e-KYC transactions shall take place using AUA/ KUA service of the Digi Yatra Ecosystem
b. All AADHAAR Related data security shall be as per the AADHAAR Act 2016
c. AUA/KUA guidelines issued by UIDAI shall be followed from time to time
d. Protocol for data exchange between KUA and CIDR database would be based on AUTH API 2.5 and above as defined by UIDAI
e. KUA would use only STQC/UIDAI certified registered devices for the purpose of reading Biometric Data
f. AADHAAR References as per Annexure 7

NB:

1. **Biometric Data Captured for Identity Validation using AADHAAR Verification cannot be stored or Reused as per the AADHAAR Act.**
2. **Use of AADHAAR will be solely for Identity Validation, which will be subject to the prescribed guidelines of UIDAI from time to time.**

GUIDELINES FOR AIRLINES, OTAS AND OTHER STAKEHOLDERS

1. Digi Yatra ID Travel Credentials are shared directly by the passengers to the relevant stakeholders and should not be a part of the Barcode/ Mobile QR Code of the Ticket or the Boarding Pass to prevent any inadvertent loss or leakage

    a. The Digi Yatra ID data shall be stored with similar data protection and privacy as applicable for other demographic data of passengers in Airline database as part of the web service call, this information will then be sent to Airports' DYBBS.

2. Airlines shall share with the Digi Yatra Biometric Boarding System (DYBBS) of the Airport the PNL data for all flights, the concerned parties shall mutually agree on a secure data sharing with Airport DYBBS

3. Airlines, OTAs and various portals maintain the Passenger phone number, Email ID, Digi Yatra ID etc. The crucial aspect of data sharing protocols amongst travel portal, airlines, airports etc. would require to be defined in secured and stringent manner to prevent data breach as mentioned in the DYBBS CYBER SECURITY REFERENCE ARCHITECTURE AND RECOMMENDED BEST PRACTICES section as given below in this Document

4. Data privacy norms for the Digi Yatra ID shall be applicable as per the IT Act 2000 and IT Amendment Act 2008 and the AADHAAR Act 2016 as relevant

5. With the consent of the Airline, Any Security Agency, GOI or other Govt. Agency may be given access to the Passenger Data based on the current/ existing Protocols prevalent at that time

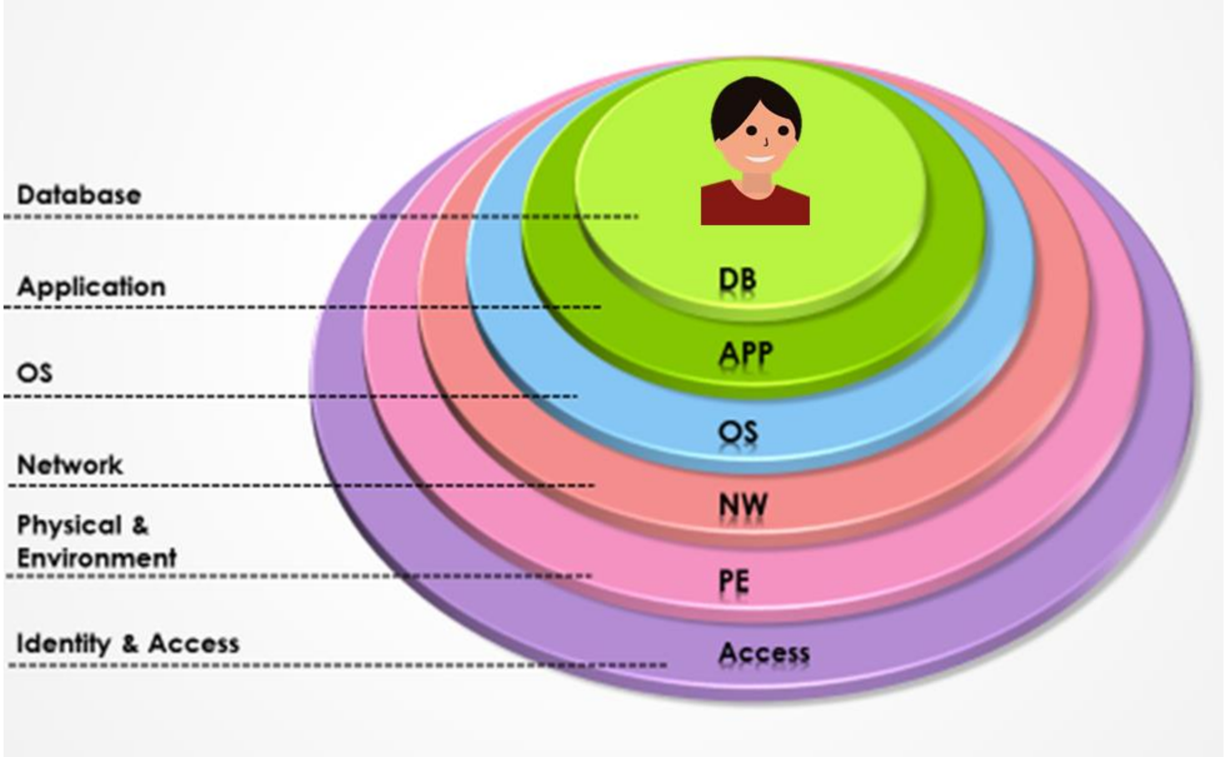
6. Digi Yatra ID Travel Credentials will be stored in the database of the airline and/ or the OTA, Airports etc. and they shall maintain the integrity and privacy of the data and protect the same as per GOI, IT Act 2000 and IT Amendment Act 2008/ Similar data protection and privacy as applicable for other demographic data of passengers in the airline database

7. The Ticket or the Boarding Pass and the Barcode/ QR code therein, shall conform to IATA standards (IATA Resolution 792)

8. Digi Yatra ID Travel Credentials will not be displayed either on the Ticket or on the Boarding pass
    a. It shall also not be coded into the Barcode barcode/ Mobile QR Code of the Ticket/ Boarding Pass

9. The Airport operator Digi Yatra Biometric Boarding System (DYBBS) will retain the Travel Data including the Digi Yatra ID Travel Credential for a duration of 30 days from the date of travel after the Passenger’s Flight departs for the purpose of any audit/ forensic analysis by BCAS or any authorized Govt. of India agencies

10. Airlines, OTAs and other Ticket Booking agents shall be subject to Audits as per the standards prescribed in the UIDAI Act 2016 and any other as mentioned in this Policy Document



1. Identity and Access Management

Streamlining the provisioning, management and monitoring of user access across all systems, shall be achieved by using directory systems such as active directory. This can be further enhanced and controlled by the extension to identity-based micro segmentation systems.

This will avoid inadequate authentication and authorization mechanism that can lead to loss/ leakage of PID (Personal Identifiable Data)

The proposed solution should have functionality for –

a. Privilege Access Management
b. Biometric based multi-factor authentication
c. Single Sign-on
d. Monitor Activity and Enforce Policy
e. Provisioning and Governance

2. Network Intrusion Detection and Prevention

Enabling detection and prevention measures for network-based intrusions. These may be implemented in standalone network appliances or as a feature of next generation firewalls. Advance or zero-day cyber-attacks can bring the entire Digi Yatra Biometric Boarding System (DYBBS) system down and cause severe business continuity issue that is not acceptable in the aviation environment. The Digi Yatra Biometric Boarding System (DYBBS) solution should have below functionality –

1. Next-Generation Firewall, in physical or Digi Yatra ID form, classifies all traffic – including encrypted traffic – and enforces policies based on applications, users, and content without sacrificing performance.
2. All threats' analysis service to dynamically analyze suspicious content in a Digi Yatra ID environment to discover zero-day threats.
3. Threat Prevention includes IPS, malware protection, DNS sinkhole, and command-and-control protection, Gateway Antivirus, Geography based blocking to block threat nations.
4. URL Filtering continually updates new phishing and malware sites, as well as sites associated with attacks, even blocking malicious links in emails.

3. Network Segmentation and Firewalling

Separation of logical IT assets into security zones reflecting the value of the information being protected as determined by the business. The principal purpose of network segmentation is to prevent network traversal of malware, advanced persistent threats or malicious actors between less sensitive environments and more highly sensitive ones. Software defined micro-segmentation provides more granularity and ease of management than physical network segmentation. Note that VLANs are not a secure means of segmentation. For example, the e-gate and kiosks at the airports or even the entire IT network need to be segmented properly to mitigate the risk of a breach happening on one environment traversing to the other. Also making e-gates/kiosks/Baggage system Digi Yatra ID segmented (and cloaked) on the same physical network will make hacking much more difficult. The solution should have below functionality –

a. Solution provides software equivalent of physical separation of devices/systems that are located in different microsegments on the same network.
b. Devices/systems in different microsegments are mutually undetectable by ping/port scanning or other network techniques.
c. Granularity of segmentation is down to the individual endpoint and user.
d. Endpoints may be located in datacenter network, Digi Yatra ID network, remote offices, private or public cloud.
e. Supports mobile device endpoints / BYOD.
f. Protects networked endpoints running any operating system or embedded system. Includes, but is not limited to, Windows, Linux, UNIXes, Mac OS, mainframe OS, embedded systems such as printers, IoT devices, SCADA systems.

g. Users may be assigned to microsegments. User identity is defined and authenticated by common directory systems such as LDAP, Active Directory.
h. Supports integration with common SIEM solutions for monitoring, alerts and exception reporting.
i. Supports encryption of data-in-motion from segmented endpoint to endpoint and should supports automated creation and teardown of encrypted tunnels
j. Supports perfect forward secrecy, i.e. past sessions protected against future compromise of secret keys or passwords.
k. Supports encryption of all IP protocols including TCP, UDP, ICMP etc.

4. Physical and Environmental Security

Physical and environmental protection of information assets using appropriate mechanisms, including:

a. Video surveillance and recording
b. Site and data center access management
c. Temperature and humidity controls
d. Situational Awareness solution for centralized dash boarding

5. Network Access Control

Restriction and control of the admission of network devices, both wired and wireless, onto the enterprise network. Modern solutions integrate with identity management systems to authenticate devices through service accounts or digital certificates.

6. OS Security

This encompasses a number of principles:

a. Hardening Operating Systems based on defined procedures
b. Reviewing OS security based on server risk profiles
c. Implementing necessary controls e.g.
d. Malware protection
e. Host-based firewalls
f. Network cloaking

7. Application Firewall

Protecting against attacks and intrusions to systems at layer 7. Typically implemented as a network appliance or as a feature of network load balancers.

8. Database Security

Database hardening, access control to databases, tables and fields based on information classification, encryption, monitoring and review of access. In the Digi-Yatra program, the PII data will be stored in the database for a short period while Passenger is still at the airport, so it is extremely important to have strong security control for database. The demographic data / Passenger Check in information data with Digi Yatra ID shall be masked to ensure security and privacy. The server storing data shall not be connected to internet/WAN/Cloud except for Airline DCS through a secured environment.

9. Data Encryption

Data encryption (biometric and biographic) both at rest and in transit is key for the Digi-Yatra program. The biometric data once lost cannot be changed as it is tied to the physiological properties of the individual. Following are some of the key factors that should be considered around encryption -

a. Encrypting sensitive data at rest
b. Encrypting data in motion either over the Internet or untrusted network segments, including wireless, to prevent eavesdropping.
c. Supports encryption of data-in-motion from segmented endpoint to endpoint.
d. Supports industry-standard encryption algorithms and protocols compliant with NSA Suite B.
e. Supports automated creation and teardown of encrypted tunnels
f. Supports automated re-keying of tunnels on specified schedule.
g. Supports perfect forward secrecy, i.e. past sessions protected against future compromise of secret keys or passwords.
h. Supports encryption of all IP protocols including TCP, UDP, ICMP etc.
i. Supports encryption of IPv4 and IPv6 traffic.
j. Supports NAT/PAT traversal of encrypted traffic.
k. Supports definition of unencrypted traffic paths.

10. Secure Wireless

Securing wireless deployments. Ensuring that all corporate access is encrypted and separated from any guest access. The proper segmentation of business and guest Wi-Fi network to be done and the integration with Network Access Control.

11. Secure Remote Access

Ensuring that all remote access is provided on a 'need to know' basis and using multifactor authentication. All remote communication must take place over encrypted channels e.g. Digi Yatra ID Private Networks. For example, if any trouble shooting, servicing or maintenance activity for any airport infrastructure or IT component is required and secured remote access should be provisioned.

12. Web and Mail Content Inspection and Delivery

Sanitizing inbound mail and web content e.g. detection and removal of malware, malicious links etc. This would mitigate the risk of an internal user unknowingly clicking on a malicious link (via email or web). This is one of the most common attack vectors as human is the weakest link in the security chain. If a user inadvertently clicks on a malicious link it can affect the entire network pretty fast and hence segmentation of the environment in addition to the content inspection solution should be put in place.

13. End User Education & Cultural Change

Frequent end user education to teach the basics of cyber security as people tend to be the weakest link in the security chain. Facilitate cultural change so that security is built into the DNA of the organization and seen as an enabler rather than an inhibitor.

14. Vulnerability and Patch Management

Proactive detection of vulnerabilities, through scanning and penetration testing in systems and applying relevant patches before vulnerabilities can be exploited. Vulnerability analysis and penetration testing are important phases within the cybersecurity lifecycle and allows an organization to understand the key security risks they are exposed to.

LOGS, METRICS AND DASHBOARDS

TECHNICAL LOGS: TIME-STAMPED TECHNICAL DATA, EVENTS & ALARMS

Operational logs like but not limited to:

- ID End Point
- Timestamp
- Nationality
- Gender
- Date of Birth
- Age
- Number of biometric captures
- Biometric capture quality score
- AADHAAR authentication result
- AADHAAR authentication process time
- Biometric Matching Score
- Matching Result
- Biometric identification time
- BCBP type
- BCBP process time
- Booking reference validation result
- Booking reference validation process time
- Complete process time
- Boarding DCS result
- Boarding DCS process time
- Processing step result

TYPICAL REPORTS

- Number of transactions (per type, status)
- Endpoint statistics (per Endpoint)
- Transaction duration
- Total number of Transactions terminated due to Operational Reasons / Total number of Terminated Transactions
- Total number of Transactions terminated due to Technical Reasons / Total number of Terminated Transactions
- Usability /Ergonomics (number of attempts for captures)
- ID usage (quantity of Identity document per type)
- Exceptions Reports (number of interventions required)

METRICS AND DASHBOARDS

- Passenger wise details should display Passenger flow between various checkpoints
- Airline wise details should display no of Passengers for that particular airline at various checkpoints
- Identify the local of Passenger in a particular zone
- Passenger dwell time between various checkpoints & at various checkpoints
- Flight wise details should display no of Passengers for that particular flight at various checkpoints
- Health monitoring of all devices at all checkpoints

DIGI YATRA FOR PASSENGERS WITH SPECIAL NEEDS & SENIOR CITIZENS

GENERAL POLICY COMPLIANCE

a. For the Purpose of catering to the needs of PRM passengers and Passengers with special needs, there will be an exception handling gate, where Passengers will be processed at all the processes at the airport from Airport Entry to the Boarding gate

b. In addition to Government of India guidelines compliance; the DY-BBS must incorporate digital accessibility features as well as comply to all parameters of international accessible standard WCAG2.0 Level AA compliance

c. DY-BBS shall ensure that digital inclusion is incorporated in using digital guidance systems, interactive kiosks and augmented reality apps enabling citizen with disability and senior citizens to navigate through the airport with ease through the assistance of assistive technology on their devices.

d. DY-BBS ecosystem partners shall ensure that digital accessibility is incorporated in the web portal, mobile apps, kiosks etc. enabling person with disability and senior citizens to access services with ease through assistive technology.

e. Kiosks should be designed such that it has the capability to integrate text to speech output enabling blind passenger to seamlessly access it with ease. (Similar to a talking ATM enabling a visually impaired customer to access the ATM independently with ease.)

f. Kiosks should enable passenger with disability and senior citizens to register themselves with ease.

g. Regional Language Kiosks should be designed in Unicode enabling passenger with disability to access these contents in regional language through their assistive technology with ease.

h. System should send an alert to airlines/ wheelchair assisting agency at the kiosks once passenger with disability checked in and places a request for assistance required for escort/ wheelchair assistance. (Note: System should be capable of taking this request at the time of booking, registration, etc.)
i. Dedicated lane for person with disability and senior citizen for Boarding gate should be assigned. System should allow more time to cross the Gate/ e-Gate in addition to 4 seconds in case of passenger with disability.
j. Process such as ticket booking, web check in, Seat selections, self-check-in through kiosks, registration at kerb side Kiosks, Digi Yatra loyalty program enrolment process, Ticket cancelation, ticket rescheduling, airport exiting process, transfer process, access to transfer kiosk should be digitally accessible enabling passengers with disability and senior citizen to access these with ease.
k. Voice guidance for capturing biometric in the system shall be provided by Kiosks (i.e. Audio beep confirming authenticated Audio voice guidance prompting user for, face in the center, face on the left, etc.)
l. Kiosks shall be placed in a manner enabling wheelchair passengers to access these with ease.
m. All information and baggage tag, passenger boarding details shall be available in digitally accessible mobile app.
n. Internal Airport map navigation should be available within mobile app and passenger with disability can be guided to boarding gate through voice guidance e.g. Google maps)
o. Digitally accessible training video should be provided online for passengers with disability highlighting guidance, registration process, check in process, request for special assistance, etc.
p. Passengers with disability who cannot be successfully verified through DYBBS should be alerted for exception verification by CISF security by the Kiosk.
q. Self-Bag Drop/Hybrid Bag Drop system should be digitally accessible enabling passenger with disability to access these with ease. In case passengers with disability are not able to access these with ease then they would comply with manual process through the assistance of AAI/ airline personnel assistance.

DIGI YATRA ECOSYSTEM: TECHNOLOGY SOLUTION

a. In this rapidly changing technological world, we would like to keep the options of us of various technology open.
b. The various options that are available are as follows.
    i. Build a Native App/ SDK with a central ecosystem

ii. Build a Native App/ SDK with a minimalistic approach without an extensive central platform and empower passengers to share data the travel credentials directly to the airlines, Airports, Immigration and other stakeholders/ agencies using W3C standards and DID protocols

iii. Build a Native App/ SDK with a backend using Blockchain Technology

AMENDMENTS TO DIGI YATRA PROCESS

The passenger processes considered in the policy are designed as per the currently available mature technologies. The implementation of this policy envisages the use of the latest technologies fulfilling the process requirement. However, it may be noted that this document will be subject to amendment from time to time to adapt the best technology and solutions available in the industry from time to time.

ANNEXURES & REFERENCES

AUTHENTICATION OF PASSENGER TO THE AADHAAR DATABASE

As per AADHAAR ACT 2016, GOI
Website: https://uidai.gov.in/images/the_aadhaar_act_2016.pdf

CUSS, CUPPS & WEB SERVICES

As per IATA standards as renewed on date:
CUSS: RP 1706c Common Use Self Service 2016
CUPPS: RP 1797 CUPPS 2016 & Web Services

BIOMETRIC ACQUISITION PRODUCTS: FINGERPRINTS READERS

AS PER ISO Standards and the latest amendments: ISO/IEC 19794-4:2017
And As per GOI recommended standards

BIOMETRIC ACQUISITION PRODUCTS: FACE READERS

AS PER ISO Standards and the latest amendments: ISO/IEC 19794-5:2011
And As per GOI recommended standards

BIOMETRIC ACQUISITION PRODUCTS: IRIS READERS

AS PER ISO Standards and the latest amendments: ISO/IEC 19794-6:2011
And As per GOI recommended standards

FRONT END DEVICES (E-GATE AND KIOSKS)

As per IATA Standards

BOOKING AND CHECK-IN STANDARDS

As per IATA Standards, Resolution 792. Annexure-1, 2 & 2A

API ECOSYSTEM

As per the IATA “Simplifying the Business” STB guidelines Annexure-3

PRIVACY BY DESIGN FUNDAMENTAL PRINCIPLES

Credits to IAB. URL: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

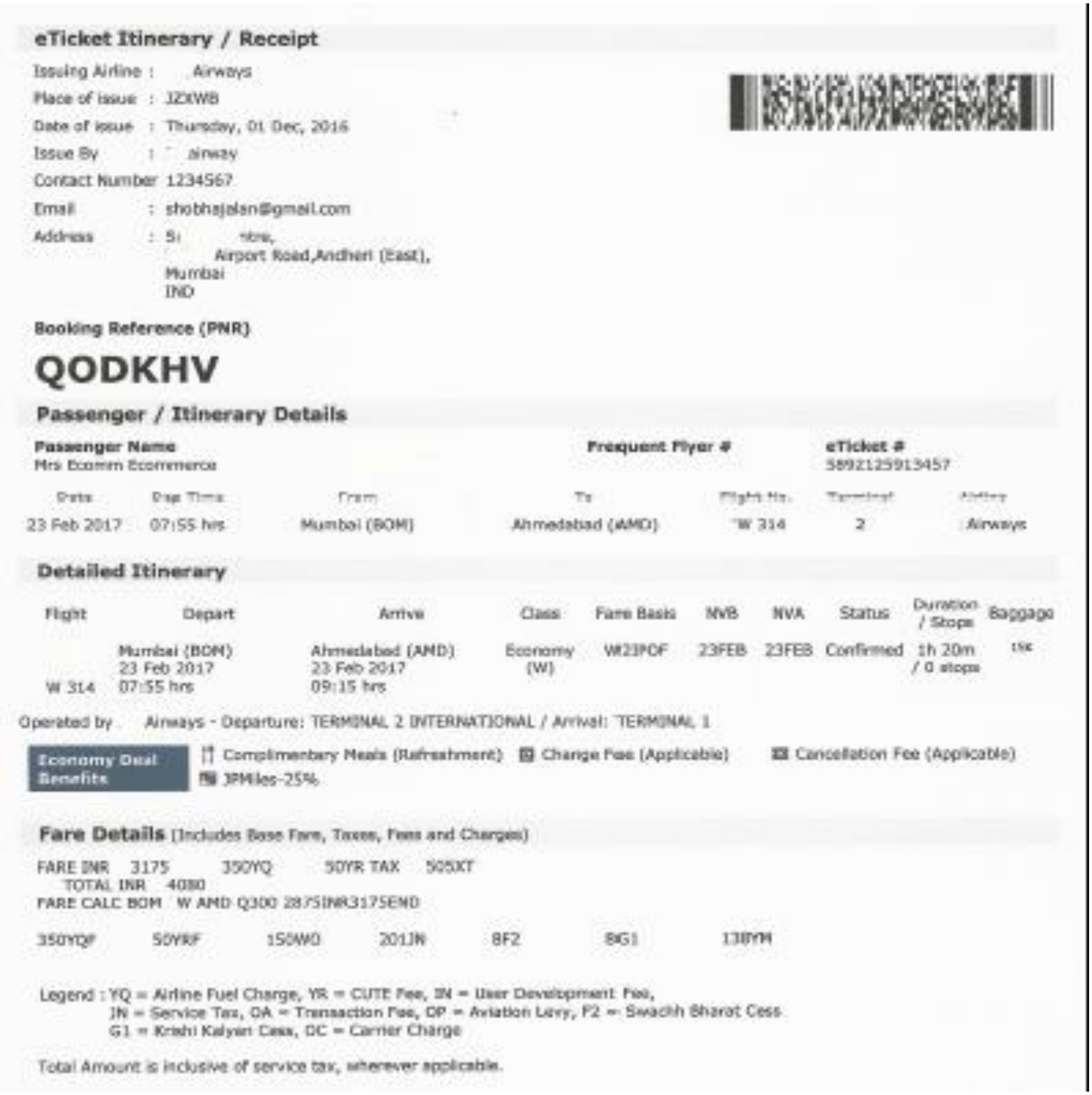
PREPARED BY:

THE TECHNICAL WORKING COMMITTEE

DIGITAL CELL

MOCA, INDIA

ANNEXURE-1: ETKT WITH BARCODE



eTicket Itinerary / Receipt

Issuing Airline : Airways
Place of issue : JZXWB
Date of issue : Thursday, 01 Dec, 2016
Issue By : airway
Contact Number 1234567
Email : shobhajalan@gmail.com
Address : S ntre,
Airport Road,Andheri (East),
Mumbai
IND

Booking Reference (PNR)

QODKHV

Passenger / Itinerary Details

Passenger Name	Frequent Flyer #	eTicket #
Mrs Ecomm Ecommerce		5892125913457

Date	Dep Time	From	To	Flight No.	Terminal	Airline
23 Feb 2017	07:55 hrs	Mumbai (BOM)	Ahmedabad (AMD)	W 314	2	Airways

Detailed Itinerary

Flight	Depart	Arrive	Class	Fare Basis	NVB	NVA	Status	Duration / Stops	Baggage
W 314	Mumbai (BOM) 23 Feb 2017 07:55 hrs	Ahmedabad (AMD) 23 Feb 2017 09:15 hrs	Economy (W)	W23POF	23FEB	23FEB	Confirmed	1h 20m / 0 stops	15K

Operated by Airways - Departure: TERMINAL 2 INTERNATIONAL / Arrival: TERMINAL 1

Economy Deal Benefits Complimentary Meals (Refreshment) Change Fee (Applicable) Cancellation Fee (Applicable) JPMiles-25%

Fare Details (Includes Base Fare, Taxes, Fees and Charges)

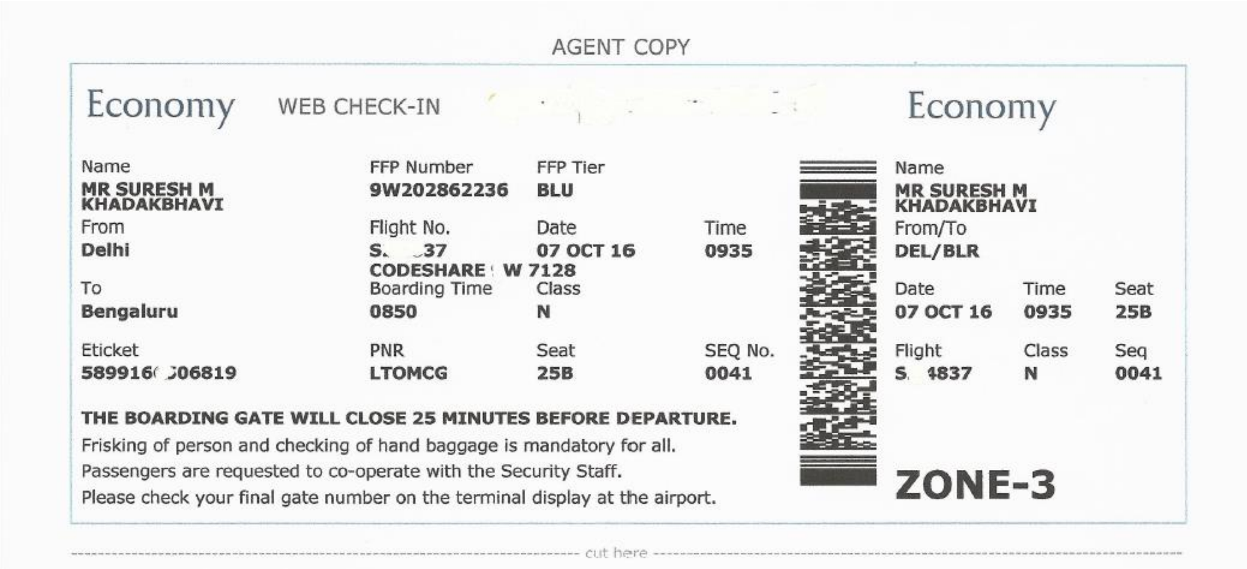
FARE INR 3175 350YQ 50YR TAX 505XT
TOTAL INR 4080
FARE CALC BOM W AMD Q300 2875INR3175END

350YQF 50YRF 150WO 201JN 8F2 8G1 138YM

Legend : YQ = Airline Fuel Charge, YR = CUTE Fee, IN = User Development Fee,
JN = Service Tax, OA = Transaction Fee, OP = Aviation Levy, F2 = Swachh Bharat Cess
G1 = Krishi Kalyan Cess, OC = Carrier Charge

Total Amount is inclusive of service tax, wherever applicable.

ANNEXURE-2: BOARDING PASS



AGENT COPY

Economy WEB CHECK-IN

Name **MR SURESH M KHADAKBHAVI**	FFP Number **9W202862236**	FFP Tier **BLU**		
From **Delhi**	Flight No. **S. 37** **CODESHARE W 7128**	Date **07 OCT 16**	Time **0935**	
To **Bengaluru**	Boarding Time **0850**	Class **N**		
Eticket **589916 06819**	PNR **LTOMCG**	Seat **25B**	SEQ No. **0041**	

THE BOARDING GATE WILL CLOSE 25 MINUTES BEFORE DEPARTURE.

Frisking of person and checking of hand baggage is mandatory for all.

Passengers are requested to co-operate with the Security Staff.

Please check your final gate number on the terminal display at the airport.

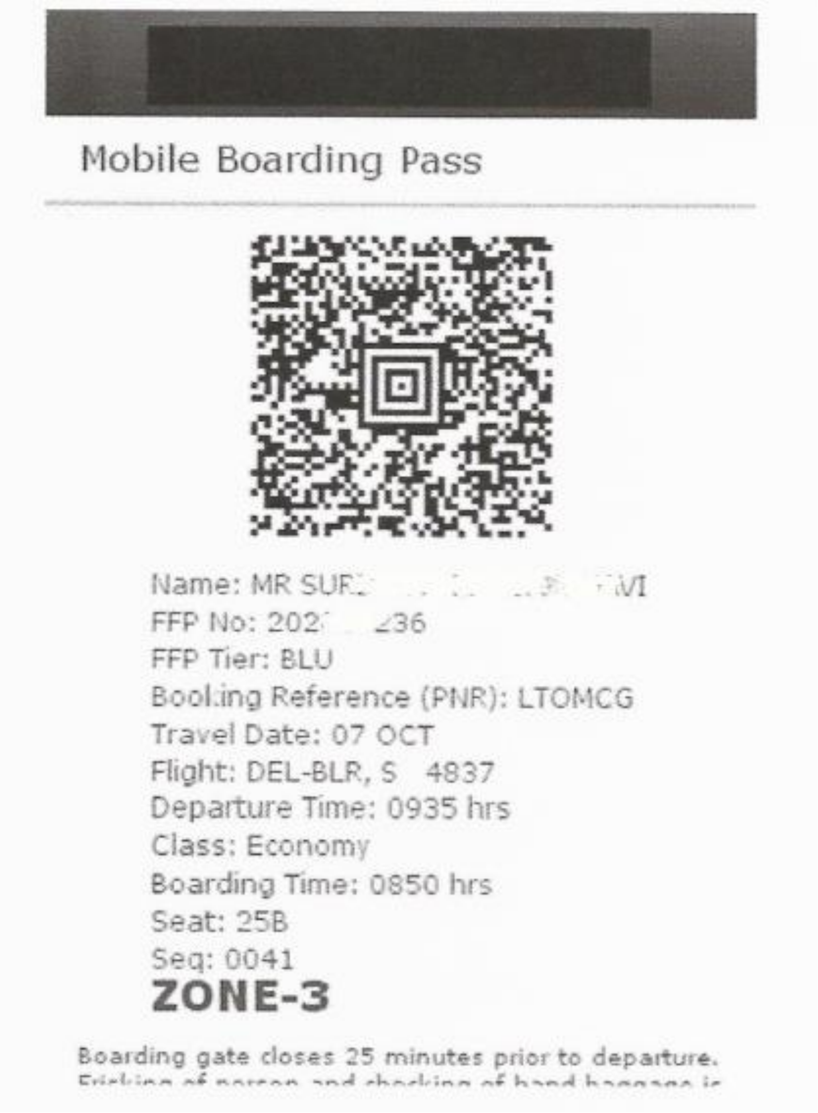
Economy

Name **MR SURESH M KHADAKBHAVI**		
From/To **DEL/BLR**		
Date **07 OCT 16**	Time **0935**	Seat **25B**
Flight **S. 4837**	Class **N**	Seq **0041**

ZONE-3

cut here

ANNEXURE-2A: E-MOBILE BOARDING PASS WITH QR CODE



[redacted]

Mobile Boarding Pass

Name: MR SUR[redacted]MI
FFP No: 202[redacted]236
FFP Tier: BLU
Booking Reference (PNR): LTOMCG
Travel Date: 07 OCT
Flight: DEL-BLR, S[redacted] 4837
Departure Time: 0935 hrs
Class: Economy
Boarding Time: 0850 hrs
Seat: 25B
Seq: 0041

ZONE-3

Boarding gate closes 25 minutes prior to departure.
Frisking of person and checking of hand baggage is

ANNEXURE-3: API ECOSYSTEM

The Open API Ecosystem shall be along the IATA STB guidelines. All Stakeholders to work over a period of time and implementation to be done by March 2019.

Open Application Programming Interfaces, commonly referred to as Open APIs, are a way to share data between entities in a trusted, timely yet open manner. The need for the entire aviation industry to share data is becoming greater every year. Initiatives such as artificial intelligence, customer personalization, and real-time operations need relevant, trusted, and timely data to operate. The vision is to use Open APIs to allow airlines and airports to communicate with Passengers and publish relevant data. Moreover, the aim is to ensure the data exposed from individual airline API platforms is consistent in terms of definition, format and the way the data is accessed (or shared).

General Purpose API					
Flight Status API	This API provides information about a particular flight like flight status (security, boarding etc), check-in counters, gates, scheduled and estimated arrival / departure times.	L1-Mandatory	AODB/ FIDS or DCS	Provided	Open
Complaints API	This API allows users to provide complaints. feedback, or suggestions to Airlines and/or OTAs NB: This is needs to be integrated with Airsewa App	L1 - Mandatory	Hosted by Airport	Provided	Airlines / OTA
Traveler API	Flight Number, Passenger Name, Unique ID, Date, time of Travel, PNR, e-Ticket Number, mobile number, status Status can be “Booked”, “Check-in”,” Passenger Validation”, “Check-in”, “Baggage Checked in”, “Security check”, “Boarding”, “Landed”, “Baggage arrived”.	L1-Mandatory	AODB/ FIDS or DCS	Provided	Open

At Airport API	Fallback: In case IMID doesn’t work, the fallback is for the Passenger to scan the e-Boarding Pass (Mobile QR Code) and the gates default to close. Therefore, every IMID scanner should periodically download the latest Passengers Manifest and have the ability to perform a verification locally.

ANNEXURE-4: REFERENCE CHECKLIST

SRN	Item	URL
1.	Reference for WCAG2.0	https://www.w3.org/TR/WCAG20/ https://www.w3.org/WAI/intro/wcag https://www.w3.org/WAI/WCAG20/glance/
2.	Example of Government implementation in digital Accessibilities	1.8 Accessibility | Guidelines For Indian Government Websites
3.	Developing Accessible IOS mobile App	https://developer.apple.com/library/content/documentation/UserExperience/Conceptual/iPhoneAccessibility/Introduction/Introduction.html
4.	Developing Accessible Apps for Android	https://developer.android.com/guide/topics/ui/accessibility/apps.html
5.	WCAG2.0 standard for mobile apps	http://www.w3.org/Mobile/mobile-web-app-state/
6.	Universal accessible design Government of India portal	http://www.incometaxindiaefiling.gov.in http://www.irctc.co.in http://www.socialjustic.nic.in

ANNEXURE- 5: UIDAI REFERENCES AS PER UIDAI WEBSITE

UIDAI Documents

https://uidai.gov.in/resources.html

Authentication Overview:

https://uidai.gov.in/authentication/authentication-overview.html

Authentication Service Agencies:

https://uidai.gov.in/authentication/authentication-partners/service-agency.html

Authentication Request Agencies:

https://uidai.gov.in/authentication/authentication-partners/user-agency.html

Authentication Devices:

https://uidai.gov.in/authentication/authentication-devices-documents.html

ANNEXURE- 6: LIST OF ABBRIEVIATIONS

Abbreviation	Full form	Remarks
MoCA	Ministry of Civil Aviation	
BCAS	Bureau of Civil Aviation Security	
CISF	Central Industrial Security Force	
IATA	International Air Transport Association	
DY	Digi Yatra	
One-ID	IATA global program on document free passenger process based on Identity management and biometric recognition	
LCCs	Low-cost carriers	
FDI	Foreign Direct Investment	
TWC	Technical Working Committee	
SME	Subject Matter Experts	
AAI	Airport Authority of India	
OTA	Online Travel Agents	
CAR	Civil Aviation Requirements	
SOPs	Standard Operating Procedures	
JVC	Joint Venture Company	
SDK	Software Development Kits	
UIDAI	Unique Identification Authority of India	
SPV	Special Purpose Vehicle	
PESC	Pre-embarkation Security Check	
ABC	Automated Border Control	
ETKT	electronic ticket	
BCBP	Bar Coded Boarding Pass	
QR code	Quick Response code	
e-KYC	Electronic Know Your Customer	
INT	International	
DOM	Domestic	
DYBBS	Digi Yatra Biometric Boarding System	
AADHAAR	***AADHAAR*** is a verifiable 12-digit identification number issued by UIDAI to the resident of India for free of cost	
PNR	Passenger Name Record	
PNL	Passenger Name List	
DCS	Departure Control System	
CUSS	Common Use Self Service	
SSBD	Self Service Bag Drop	
DFMD	Door Frame Metal Detector	
SHA	Security Hold Area	
GDS	Global Distribution System	

IR	Infra-Red	
UV	Ultra-Violet	
PSP	Passport Seva Project	
IVFRT	Immigration, Visa and Foreigner’s Registration and Tracking	
FRRO	Foreigners Regional Registration Officer	
CPU	Central Processing Unit	
API	Application Programming Interface	
STQC	Standardisation Testing Quality Certification	
CERT-In	***CERT-IN*** is the national nodal agency for responding to computer security incidents as and when they occur.	
DPIA	Data Protection Impact Assessment	
DPbD	Data Privacy by Design	
GOI	Govt. of India	
BYOD	Bring Your Own Device	
VLAN	Virtual Local Area Network	
PID	Personally Identifiable Data	
PII	Personally Identifiable Information	
IoT	Internet of Things	
SCADA	Supervisory Control and Data Acquisition	
LDAP	Lightweight Directory Access Protocol	
SIEM	Security information and event management	
WCAG	Web Content Accessibility Guidelines WCAG, the globally recognized guidelines for creating accessible digital experiences from the World Wide Web Consortium (W3C).	
W3C	World Wide Web Consortium	