Airports Authority of India

Directorate of Information Technology

Safdarjung Airport, New Delhi - 110003

No. AAI/CHQ/ITD/ATD/2024

Date: 30.12.2024

Request for Budgetary Offer

Implementation of

Travel Document Authentication at 44 Airports

PAGE LEFT BLANK

Table of Contents

1. Request for Budgetary Quotes: 5
2. Introduction: 5
3. Tentative High-Level Architecture of the Central Application: 7
4. Worksites: 14
5. Project Implementation Model: 15
6. Scope of Work (SoW): 16
7. Scalability: Design of Scale 19
8. Tentative Project Tenure 21

Annexure – I: Tentative Hardware Specification 22

Annexure – II: Sample Components of IATA 792 Standard 24

Annexure – III: Budgetary Quote Submission Format 26

PAGE LEFT BLANK

1. Request for Budgetary Quotes:

1.1. Airports Authority of India (AAI) intends to invite Budgetary Offers from Prospective Bidders for **'Implementation of Travel Document Authentication at 44 Airports'**.

1.2. This Budgetary Offer is called to assess the tentative cost to implement the aforesaid solution as per the BoQ provided under Annexure – III.

1.3. The Budgetary Offer should be submitted on or before **21 Jan, 2025**.

1.4. AAI reserves the right to add, modify, amend or delete any of the requirement, as mentioned in this document for Budgetary Offer, at the time of tender.

1.5. The document is for budgetary purpose only. Work shall be awarded following the laid down procurement process of AAI.

1.6. For queries related to the Budgetary Quote, the prospective bidders are advised to send request for clarifications, if any, through email at skmit@aai.aero only.

2. Introduction:

2.1. For implementation of this project, AAI is looking to leverage the best in digital technology to deliver seamless experience to its passengers. This project will also focus on achieving operational efficiencies and security effectiveness for its key stakeholders such as Passengers, Airlines, Airport staff and CISF.

2.2. Standards and Guidelines:

2.2.1. Travel Document Authentication (TDA) shall be primarily carried out as per "AvSec order 7/2024 dated 30.04.2024 issued by Bureau of Civil Aviation Security (BCAS)", and amendments thereof.

2.2.2. The applicable Guidelines as per "IATA Resolution 792 for Bar Coded Boarding Pass (BCBP)", and amendments thereof, shall provide the basis of implementation as well.

2.2.3. Indian Law, including but not limited to Information Technology Act 2000, Information Technology Amendment Rules of 2023 and Digital Personal Data Protection Act, 2023; along with any other applicable guidelines/ rules/ regulations issued by appropriate Authority shall be followed in the project.

2.3. Ownership of the Solution and Bespoke Development:

2.3.1. AAI is looking to develop a comprehensive solution for Travel Document Authentication (TDA) process where the ownership & Intellectual Property Rights (IPR) of the entire Solution will be with AAI.

2.3.2. The entire solution is envisaged to be developed in a bespoke development model, where the source code, object code, configuration and all other relevant materials, artefacts etc. of all bespoke development shall be the property of AAI and AAI shall own all Intellectual Property Rights (IPRs) for them. All material related to such bespoke development shall be treated as confidential information. Bidder shall have no right to market/ sell the software, without prior written permission of AAI.

2.3.3. AAI acknowledges the need for usage of certain Commercial-off-the-Shelf (COTS)/ Proprietary/ Open Source Products which may provide basis for the required Bespoke Development of the solution, such as OS, Anti-Virus, Database etc. For cases where usage of such Commercial-off-the-Shelf (COTS)/ Proprietary/ Open Source Products is the only option to meet the Project Requirements, Perpetual & Unlimited Licenses, free from any kind of limitation in terms of usage, time period or any other conditions, may be provided only with prior written approval of AAI.

2.3.4. The ownership of all hardware and licenses required for the Project shall be with AAI. All necessary Licenses must be provided on or before Go-Live of the Solution, sufficient in all respect to satisfy the offered solution for the entire duration of the Project.

3. Tentative High-Level Architecture of the Central Application:

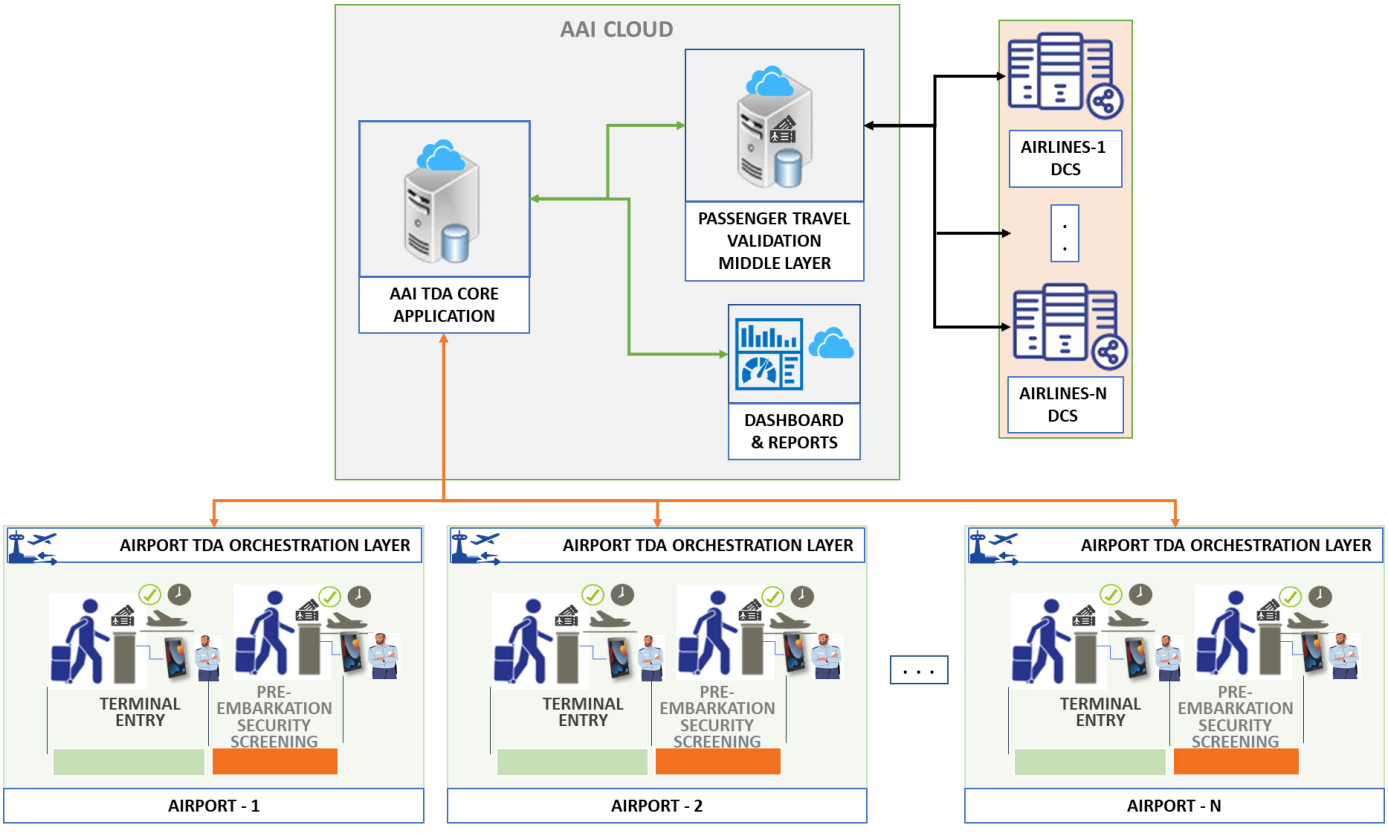
3.1. The proposed system must be a centralized cloud-based solution, including but not limited to the Layers/ Modules described hereunder.

3.2. It must be able to cater to all departing passengers, including both domestic and international, for all operating airlines at all AAI Airports, without any restriction or limitation whatsoever.

3.3. Appropriate provision to scale the solution as per AAI Operational requirements must be incorporated. The architecture must be capable of being scaled up to handle more user requests or more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

3.4. The High-Level Architecture described below is only a tentative Draft to further explain the Scope of the Project. It may be suitably modified by Prospective Bidders to achieve the desired functionalities.

3.5. High-Level Architecture Diagram:



3.6. High-Level Description of Central Travel Document Authentication (CTDA) Application Modules:

3.6.1. <u>Module 1: Airport TDA Orchestration Layer</u>

This Layer will facilitate/ orchestrate validation of Travel Credentials, i.e. Physical Tickets, e-Tickets (both in printed and digital format) and Bar-Coded Boarding Pass (BCBP), with Airlines Departure Control System (DCS) for all Departing Passengers at each Airport.

a. This Layer aims to provide a hassle-free passenger processing through different touchpoints at the Airports, such as Terminal Entry Gates, Pre-Embarkation Security Check (PESC).
b. It shall be enabled for all Departing Passengers, **both Domestic and International**.
c. This Layer must provide a level of abstraction to integrate with all required Hardware at any Airport.
d. The System must also be capable of expansion to other touch points at the airports and all AAI Airports, as per AAI Operational Requirement.

3.6.2. Module 2: Passenger Travel Validation Middle Layer

This Layer will integrate with the Departure Control Systems (DCS) of all Airlines to collect all PNR/ PNL Details, Flight Details other relevant fields to validate Travel credentials of Passengers.

a. All operational airlines, including Domestic and International, must be to onboarded and their respective DCS must be integrated. System must use either API/ MQ/ XML/ any other data exchange format, specific to airline's requirement, in order to maintain Airlines Data, PNR/ PNL Data and other relevant fields required for AAI operational requirement.
b. System design must be designed to ensure that data is synchronized in near real-time basis with the Airline DCS till the departure of scheduled journey (denoted by T), i.e. T-24, T-12, T-6, T-5, T-4, T-3 and then in every 3 minutes till T-0. Any changes at DCS must be immediately pulled into System, irrespective of the synchronization window.
c. System design must be able to purge Passenger Name List (PNL) data within 24 Hours of departure of flight. System logs, Audit Trails and Statistical Data must be retained.
d. Once a passenger reaches at any Airport touchpoint, the PNR/ PNL Data of the Passenger will be validated through this layer to verify passenger Travel credentials.
e. Dedicated APIs must be developed for this module, which can be used to perform any kind of Passenger Validation/ Reconciliation/ Generation of Statistical Information etc. for this project or any other project within AAI, with no additional financial implication.
f. This Layer shall be able to cater to all departing passengers, including both domestic and international, for all operating airlines at all AAI Airports, without any limitation, restriction and additional financial implication.

3.6.3. Module 3: AAI TDA Core Application

This Layer will act as the core decision making layer of the proposed system. All business logic must be incorporated in this layer for seamless verification of Passenger Travel Credentials.

a. This Layer shall be integrated with all other Layers/ Modules as described above and the Central Dashboard & Reports System.
b. The basic objective of this Layer is to obtain all necessary inputs from different Layers/ Modules, process them through the required Business Logic and provide necessary output/ decisions to different Layers/ Modules.
c. This Layer should act as the Data Source for required Project Dashboard and Analytics is to be present in this layer, i.e. all Statistical Data, Audit Trails, System Logs and SLA Monitoring Details should be available in this Layer. Hence, all automated monitoring tools

deployed for the project, must also be integrated with this Layer to provide real-time details.

d. Passenger re-conciliation data for all passenger processed through Airport TDA Orchestration Layer must be maintained in synchronized manner for each departing flight of each Airport.
e. This Layer shall be able to cater to all departing passengers, including both domestic and international, for all operating airlines at all AAI Airports, without any additional financial implication.

3.6.4. Module 4: Dashboard & Reporting

This Layer will act as the central Business Intelligence and Dynamic Dashboarding Layer as per AAI operational requirement and must be capable to generate report in HTML/ PDF/ CSV format.

a. This Layer shall be integrated with the Core Application Layer and shall provide a Single Platform for all types of Statistical Data Reporting, Automated SLA/ Compliance Monitoring, Audit Trails Monitoring, System Log Monitoring etc.
b. This Layer should have the capability to provide API based integration for data exchange (unidirectional and/or bidirectional) with AAI website or other external systems.
c. This layer must provide Real-Time information, customized as per AAI requirements, through an easy to use, visually clean and uncluttered web-based GUI.
d. This layer must provide dynamic Data Selection, Aggregation and result filtration mechanism to generate custom reports, in addition to the regular reports configured in the layer.

3.7. Key Points to be considered in the System Architecture:

3.7.1. Bidder must develop the Central Travel Document Authentication (CTDA) Application in such a manner that it is not hardwired to any vendor algorithm. It must be ensured to include following qualities as built in feature of the system as per modern-day best practices:

a. Identification of current and provisioning for potential Users of the System
b. Digital Access and Delivery Mechanisms
c. Service Oriented & Modular Architecture
d. Alignment to MVC (Model View Controller) Design Pattern
e. Alignment to Privacy by Design Principles
f. End to End Security
g. Open Integration Framework
h. System Management & Support
i. Data store partitioning
j. Improved Performance & Response Time
k. Automated Health Monitoring & Alerts

3.7.2. Key Points to be considered in system architecture are appended below:

Sl.	Parameters	Key Points
A	General Guidelines	**1.** The solution design must be based on open industry standards and protocols. **2.** The solution must be centrally deployed and globally accessed. **3.** The solution must be modular, scalable and flexible as a true 'Cloud Deployable' solution. **4.** The solution must provide interoperability across Cloud Providers, Platforms. **5.** Bidder will design the system as a platform that can easily be replicated across airports as and when required. Also, the system must be scalable and resilient.
B	Dedicated Solution	**1.** The entire solution, including its components, such as Software, Middleware, Hardware, Network, Connectivity etc. must be dedicated for this project. **2.** The entire solution must be architected to work and achieve its functional objectives in isolation from any other existing Airport infrastructure/ solution. **3.** The proposal shall be so submitted that the dedicated Solution for this project shall not be utilized to take functional leverage from any of the existing solution(s), provided by the same vendor or its partner(s) or other vendors, and vice versa, at any of the airports. **4.** However, Integration with the any existing infrastructure to achieve functional objective of this project shall be in accordance with the details provided in the following para.
C	API driven architecture	**1.** The Bidder needs to set up, operationalise and maintain system for APIs, as per the IATA 'Simplifying the Business' (STB) guidelines. **2.** The Bidder, in consultation with AAI, will be required to set up a process for issuance of standards for the System APIs. **3.** Central Travel Document Authentication (CTDA) Application must be integrated with Airlines DCS and AAI airports under considerations, through Hub & Spoke model. **4.** The bidder must integrate and exchange information, to and/or from the other systems deployed at Airports, such as DigiYatra, AODB, FIDS, CUPPS etc., as per airport operational requirement, at the sole discretion of AAI without any additional financial implication. **5.** Such exchange of information/ integration may be a batch exchange of data or live integration on a transactional basis. The utility may reside either in the external system, or in this system or both, based on requirement for data exchange and feasibility of change in respective systems. Such exchange of information/ integration may be real-time, near real-time, periodic, based on event triggers etc. **6.** Further, there may be external/other systems that may consume/ transmit data in other formats. The Bidder shall be solely responsible to build converters/ adapters to convert such data into the desired format or vice versa, without any additional financial implication. The convertors/ adapters will reside in this system and will parse the data as and when required.

Sl.	Parameters	Key Points
D	Application	**1.** The ownership of the product licenses, wherever applicable, would be with AAI. **2.** The solution design must focus on developing workflow and business transaction, rules management, configuration management. **3.** All applications must consider appropriate security, performance, efficiency and maintainability issues based on the functional, technical and non-functional requirements and the defined SLAs. **4.** The Bidder must ensure that services must be written in such a way that they can be automated for testing. Test validation is necessary to ensure services can be upgraded, re-factored, etc. without breaking other services that use them. The Bidder must ensure that all services must be inherently versioned and all invocations must specify the version of service. **5.** Bidder must ensure that new versions of services must be backward compatible with at least three previous versions so that users of the service can start using new version of the service without mandatorily making changes to their code.
E	Hardware Agnosticism	**1.** The Solution must be loosely coupled with the required Hardware. It must allow for easy addition of devices (plug and play) with minimum customization and is ready for future systems. **2.** The solution must be architected in such a way that there is no restriction on Hardware in terms of specific makes, models or pre-certifications. **3.** Any hardware, compliant to the hardware specification provided by AAI and Interface Specification evolved during the execution of the Project, must be able to work seamlessly with the Solution.
F	Support for PRM and Senior Citizen	**1.** While designing the solution and Process flow for passenger processing, Bidder must use Digitally accessible products. **2.** Suitable audio-visual or other guidance/ assistance mechanisms should be integrated with the solution to provide required accessibility features.
G	Data	**1.** Data must only be accessed through application / interfaces for create, update and delete. There must not be any direct access to the data layer for users until and unless authorized by AAI under special circumstances. **2.** Data entry in the system shall be performed in at-least 3 languages including Hindi, English and Regional language (of the respective airports).

Sl.	Parameters	Key Points
H	Data Security	**1.** Bidder shall provide strategy to maintain data security at the application level, database level, messaging level and middleware level. **2.** Bidder shall provide security strategies when the applications are accessed from outside the network or accessing resources outside the network. **3.** Bidder shall provide strategies of encryption and security for external transaction with partner network and systems. **4.** All such strategies provided by the bidder must be implemented throughout the duration of the Project, in line with the applicable Security Standards and Guidelines. **5.** Bidder must provide ISO 27701 Certification for the developed solution related to Privacy Information Management System, with no additional financial implication on AAI. **6.** Cloud Service Provider shall ensure compliance to the following standards at all times and get certification wherever applicable. Where certification is not applicable a self-compliance assessment report shall be submitted at least on an annual basis by the service provider. **7.** Following Security Controls shall be ensured for Cloud and/ or the Solution at all times - i. ISO/IEC 27017 - Security controls for cloud services. ii. Cloud security guidelines by MIETY for security and other compliance controls. iii. GDPR iv. ISO 27001:2013, Information Security Management Systems. v. ISO 27018, Information Security Protection of Personally Identifiable Information. vi. The Digital Personal Data Protection Act, 2023
I	Data Privacy	**1.** The solution must be architected with alignment to 'Privacy by Design' principle. **2.** The solution must ensure strict compliance to Law of the Land, especially Data Security and Privacy rules in vogue, including 'The Digital Personal Data Protection Act, 2023' published on 11 August 2023 and guidelines released from time to time, for entire project duration. **3.** The bidder shall be responsible for protection of all Personally Identifiable Information (PII). **4.** The Bidder shall be Data Fiduciary for all transactional Data, including Personal Identifiable Information (PII) data. However, AAI shall retain the rights to access such data, if needed. **5.** AAI shall be Data Fiduciary for all Statistical Data, including but not limited to usage statistics, audit logs, configuration, access control logs and metadata of the entire project. The contractor shall act as Data processor for such type of data.

3.8. Cloud Deployment:

3.8.1. Bidder must architect an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) or both IaaS and PaaS on Virtual Private Cloud (VPC) / Government Community Cloud (GCC) deployment model (as per MEITY) of a MEITY empaneled Cloud Service Provider. In case of GCC model also, Central Application and infrastructure stack must be logically segregated from the other Government clients.

3.8.2. The bidder must deploy the Solution in both Data Center (DC) and Disaster Recovery (DR) site. The database layer for the Solution shall be deployed in N+N High Availability mode. The Web and Application layer for solution shall be deployed in N+1 High Availability mode (Active-Active).

3.8.3. DC & DR must be provided by the same CSP. The CSP must specify DC and DR locations. Both must be physically located within INDIA.

3.8.4. The Cloud Service Provider (CSP) must support BYOL (Bring your own license). The OS offered must come with continuous updates and upgrades for the entire contract duration.

3.8.5. The Bidder must use Open Source Solution (Enterprise Edition) for any application software that Bidder would be deploying on Virtual Private Cloud/ Government Community Cloud of CSP.

3.8.6. Bidder must provide network information of cloud virtual resources & its utilization (i.e. CPU graphs of each cloud virtual machine) from CSP to AAI.

3.8.7. Bidder must offer provision to monitor latency to cloud virtual devices resources from CSP to AAI.

3.8.8. The CSP must offer block storage volumes greater than 1 TB in size.

3.9. Network & Connectivity:

3.9.1. Bidder shall be responsible for provisioning of requisite network infrastructure and MPLS Bandwidth for integration between Central Travel Document Authentication (CTDA) Application, Airlines DCS and Airports in consideration.

3.9.2. Every Airport must be connected to both DC and DR. There must be redundancy from two different service provider for the MPLS line. The bidder needs to provision for required network bandwidth to ensure no latency or performance degradation in the system.

3.9.3. The Network Bandwidth Service Provider must have capability to run IPV4 and IPV6 (dual stack) on MPLS VPN links from date of Go-Live. Upgrade to IPV6, if required, will have to be without additional financial implication to AAI.

3.9.4. Bidder shall be responsible to provide and establish all Network requirements, including but not limited to, cabling, conduiting, etc. for the Project.

3.9.5. Bidder shall be responsible to provide last-mile power connectivity, including but not limited to, cabling, conduiting, provision of UPS (if required) etc. for the Project.

4. Worksites:

4.1. Airports to Implement Travel Document Authentication Facilities:

Proposed project is planned to be initially implemented at 44 Airports –

1	Agartala
2	Allahabad
3	Amritsar
4	Aurangabad
5	Ayodhya
6	Bagdogra
7	Belgaum
8	Bhopal
9	Bhubaneshwar
10	Calicut
11	Chandigarh
12	Coimbatore
13	Darbhanga
14	Dehradun
15	Dibrugarh

16	Gaya
17	Goa
18	Gorakhpur
19	Hubli
20	Imphal
21	Indore
22	Jabalpur
23	Jammu
24	Jodhpur
25	Kolkata
26	Leh
27	Madurai
28	Patna
29	Port Blair
30	Pune

31	Raipur
32	Rajahmundry
33	Rajkot
34	Ranchi
35	Silchar
36	Srinagar
37	Surat
38	Tirupati
39	Trichy
40	Udaipur
41	Vadodara
42	Varanasi
43	Vijayawada
44	Vishakhapatnam

4.2. Apart for the initial list of Airports as mentioned above, the solution may be implemented at any AAI Airport across the Country, at the sole discretion of AAI.

4.3. The lists provided above are tentative and for Budgetary Purposes only. AAI may add, update, modify, delete any Airport for the aforesaid lists during the Tender Process, at its sole discretion.

5. Project Implementation Model:

5.1. AAI Central Travel Document Authentication (CTDA) Application:

5.1.1. The CTDA Application to be developed under this project shall consist of all the required Modules/ Layers/ Systems for Travel Document Authentication, as depicted under the High-Level Architecture above, for all AAI airports under consideration.

5.1.2. One-time payment shall be made towards the efforts for CTDA Application development/ deployment on cloud including integration with external interfaces and connectivity.

5.1.3. The CTDA Applications shall have the flexibility to add/ modify/ remove airports on need basis along with its computational requirements.

5.1.4. No additional payment shall be applicable for the CTDA Application on any account, including but not limited to enabling additional airports, or adding additional touch points, or onboarding additional Airlines, or catering to additional passengers etc., except for the payments applicable as per the BoQ.

5.2. Airports:

5.2.1. New Airports may be added in the System at the sole discretion of AAI.

5.2.2. Enablement of such Airports may include efforts for, but not limited to, establishment of dual network connectivity to that Airport, establishment of required Local Network Infrastructure, provision of Edge Computation Infrastructure and/ or any other provision required to deploy/ configure the required processes at that particular Airport.

5.2.3. Payment shall be made for such efforts required to deploy /configure the Travel Document Authentication Processes at the individual airports, as per the BoQ rates, only once per airport basis.

5.3. Airport Touchpoints:

5.3.1. Any new Hardware, as per the BoQ, may be added at any existing or new Touchpoints at any AAI Airport across the Country, at the sole discretion of AAI.

5.3.2. Addition of such Hardware may include efforts for, but not limited to, addition of required licenses, addition of required cloud infrastructure, establishment of last-mile connectivity (Network and Power) to that particular touchpoint and/ or any other provision required to operationalize the touchpoint.

5.3.3. Payment shall be made for such efforts required to operationalize the individual touchpoint, as per the BoQ rates, on each touchpoint basis.

6. Scope of Work (SoW):

6.1. The SoW of the Project shall broadly include End-to-End implementation of all required Functionalities for Travel Document Authentication Processes, including Software, Middleware and Hardware required for the same.

6.2. The Travel Document Authentication Process is mandatory for all Departing Passengers, including both Domestic and International, except for those who have opted for and facilitated through DigiYatra. Any passenger, who has opted for but could not be facilitated through DigiYatra, must follow the Travel Document Authentication Process as well.

6.3. In the envisaged Travel Document Authentication workflow, the passenger terminal entry process is designed to ensure efficient and secure access, adhering to IATA 792 standards. Following are the objective of this workflow:

6.3.1. Automated Travel credentials validation –

6.3.1.1. Scanning and validation of Physical Tickets, e-Tickets and Bar-Coded Boarding Pass (BCBP) at Airport Airport entry,

6.3.1.2. Scanning and validation of Bar-Coded Boarding Pass (BCBP) at Pre-embankment Security Entry Check (PESC) & Transfer Area.

6.3.2. Manual Passenger Identity Credentials validation by CISF/ASG.

6.4. Indicative Functionalities for implementation of such processes are described in this section.

6.5. Functionalities for Travel Document Authentication Process:

6.5.1. <u>At Airport Touchpoint (Entry, PESC and Transfer):</u>

a. Airport Entry shall be facilitated through Scanner & CISF Tablet. Draft Specification of such Hardware are provided at Annexure – I.
b. Passengers shall scan their Physical Tickets or e-Tickets or Bar-Coded Boarding Pass (BCBP), either in printed or in digital format.
c. For both Checked-In and Non-Checked-In Passengers, the System validates passenger PNR against data received from Airline DCS.
d. System retrieves key passenger name(s), Flight Number, Departure Date & Time, Passenger Count, Sequence ID (optional), etc, as associated with validated PNR.
e. Post validation, adequate passenger travel credentials are Display at ASG/ CISF Tablet.
f. ASG/ CISF manually validates Passenger Identity and Passenger Name against the retrieved passenger details, to cross the touchpoint.

6.6. Key Functionalities for Travel Document Authentication Processes:

6.6.1. The System must be capable to identify Duplicate, Modified and Forged Travel Credentials, including Physical Tickets, e-Tickets and Bar-Coded Boarding Pass (BCBP)Bar-coded Boarding Pass (BCBP).

6.6.2. The system must have near real-time synchronization with Airlines DCS, i.e. from T-24, T-12, T-6, T-5, T-4, T-3 and then in every 3 minutes till T0 (Departure of scheduled journey). Any changes at DCS must be immediately pulled into System, irrespective of the synchronization window.

6.6.3. For effective passenger reconciliation, zones must be logically created for each airport which shall have the status of crossed touchpoint for each passenger according to the flight. Data clustering w.r.t to airlines should also be provisioned.

6.6.4. All relevant scenarios related to Passenger De-boarding and partial De-boarding must be handled at respective Touchpoints.

6.6.5. The system must be able to cross-verify duplicate PNR/ PNL processed either through the DigiYatra Validation or through the Travel Document Authentication Process. Specific alerts should be generated in the CISF Tablet if such duplicate processing scenario is detected.

6.6.6. Adequate logic must be implemented centrally to handle Irregular Operations (IROP) situations, De-boarding scenarios, Partial de-boarding, No-Show cases etc. for each Airport. Same must be detailed at time of design phase, during project implementation to meet all operational compliance.

6.6.7. The system must purge all Personally Identifiable Information (PII) data from the entire System within 24 Hours from the departure of the respective flight. However, System logs, Audit Trails and required Statistical Data (without any PII) must be retained.

6.7. Major Components of Travel Document Authentication (TDA):

6.7.1. The AAI Travel Document Validation Application: A centralized system to be deployed across 44 airports, hosted on “MEITY Empaneled Cloud”, for validating passenger travel credentials. Following are its Key Components:

6.7.1.1. Integration with Digi Yatra for passenger re-conciliation and duplicate processing validation.

6.7.1.2. Integration with Airline DCS to validate Passenger Travel Credentials at Airport Touchpoints.

6.7.1.3. Integration with AOCC, only for AAI AOCC airports.

6.7.1.4. Integration with FIDS, for non-AOCC Airports.

6.7.1.5. Dashboard and Reports: To provide a real-time monitoring statistic, including security alerts for mismatches or forged documents.

6.7.2. Establishing the necessary infrastructure to collect and validate passenger data and deploying the centralized travel document validation system across 44 airports. This includes integration with Digi Yatra and airline DCS for seamless real-time operations. ensures uninterrupted communication between the AAI application, DigiYatra ecosystem, and airline DCS.

6.8. Comprehensive Annual Maintenance Contract (CAMC):

6.8.1. The bidder must provide all necessary services for Comprehensive Maintenance of the Solution centrally and at all the Airports, for all components of the Solution such as Hardware, Software, Middleware.

6.8.2. The bidder must maintain all relevant Service Level Agreement (SLA) Parameters as per the agreed upon SLA.

6.8.3. Bidder shall carry out implementation of software/ firmware updates, patches, upgrades etc. periodically and as required.

6.8.4. Bidder must maintain asset, attendance maintenance and other required registers at every Airport, along with the Automated Dashboard & Reporting through the Central Application.

6.8.5. For each airport, Bidder must ensure availability of 10% critical spare of all type of hardware to be maintained on site. It must be ensured that hardware availability of service i.e. Uptime over 99.95%, 7 days/24 hours operations, measured by SLA Monitoring Tool, to be provided by Bidder with no additional financial implication on AAI.

6.8.6. To maintain Project SLA, the contractor shall provide all necessary support systems, infrastructure and technical support staff (Level 2 or above, not a daily wage worker) at individual airports. The Contractor shall comply with applicable Labour Laws and regulations issued thereof, amended from time to time, issued by appropriate authorities. Workmen Compensation Insurance shall be applicable for such deployed resources.

6.8.7. Back-to-Back Support:

a. CAMC support for all hardware shall be applicable from the date of start of CAMC, with Back-to-Back Next Business Day (NBD) support from OEM. The same should be certified by OEM with relevant documents.

b. CAMC support for all Commercial-off-the-Shelf (COTS)/ Proprietary/ Open Source Products, which have been implemented with prior written approval of AAI, shall be applicable from the date of start of CAMC, with Back-to-Back Next Business Day (NBD) support from OEM. The same should be certified by OEM with relevant documents.

c. 24X7 support for all other software/ middleware components developed under Bespoke Development Model, shall be applicable from the date of starting of CAMC.

6.9. Performance Parameters:

6.9.1. The entire Solution, including all components of the such as Hardware, Software, Middleware, Network, Connectivity etc. must have uptime of 99.95% or above, operating under 7 days/24 hours operations.

6.9.2. The Processing Time for entire Travel Document Authentication, from scanning of Travel Document at Touchpoint till the presentation of validated Travel Credentials in the CISF Tablet, must not be more than 2 Seconds.

6.9.3. Recovery Time Objective (RTO) of the entire Central Application, based on the successful operations from DR Site and restoring the services back to DC, must not be more than 15 Minutes.

6.9.4. Recovery Point Objective (RPO) of the entire Central Application, based on the successful operations from DR Site and without any Data Loss, must not be more than 5 Minutes.

7. Scalability: Design of Scale

7.1. The solution would be done keeping in mind the scalability of the system. As per AAI operational requirement, the project can be extended to any worksite/ Airport.

7.2. All components of the Solution will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort. As the Project moves to next level, where New Airports gets added to the system, the system should be scalable and robust to handle passenger traffic from additional airports. The system should be designed considering future proofing of the system for volume handling requirements.

7.3. The CTDA Application functions must be divided logically and developed as Modular solution. Solution functionality must be extended to other airport without significant impact to existing functional components and infrastructure.

7.4. The Solution must be able to support at least 30% Year on Year passenger Growth.

7.5. The System must be scalable to support changes to facial algorithms.

7.6. The system should be able to scale horizontally & vertically.

7.7. Horizontal Scalability – Airports and Infrastructure under the Project

7.7.1. Central Travel Document Authentication (CTDA) Application, along with all of its Systems, Sub-Systems, Components, Sub-Components, Modules, Interfaces, Configurations etc. will be common for all AAI Airports where the Solution may be implemented. Hence, implementation of the same must be One-Time Activity by the Contractor. During the currency of the Contract, new Airports may be added to the CTDA Application, at the sole discretion of AAI. Hence, the entire solution must be robust enough to scale it across all AAI Airports in the Country for the entire volume of Departing Passengers, both Domestic and International, if so desired by AAI.

7.7.2. During scale of the project - Airport specific infrastructure setup, SITC of all Hardware Items, especially Biometric Touchpoints (Gate or Pod), as per operational requirements of AAI and integration of the same with CTDA Application - would be recurring activities, whenever any addition/ modification is required in terms of Airports or Touchpoints. BoQ Items related to them may be executed by AAI, in whole or in part, as many times as required, to achieve its operational objectives.

7.7.3. It is expected that the contractor – based on the growth in terms of number of Airports, Touchpoints and the user load – will provide and scale up the Cloud Infrastructure including compute, memory, storage and bandwidth requirements to support the performance requirements of the solution and meet the SLAs. Any such scaling up would be the responsibility of Contractor during the currency of the contract, without any additional financial obligation to AAI.

7.7.4. It is expected that the contractor – based upon increase in operational airlines at all airports under the contract – will provide and scale up the CTDA Application, integrated with Departure control System (DCS) of airlines on cloud along with storage, API changes and networking

requirements. Any such scaling up would be the responsibility of Contractor during the currency of the contract, without any additional financial obligation to AAI.

7.8. Vertical Scalability – Time Span of the Project

7.8.1. System must be architected to sustain at least 10 years from Go-Live, which includes 01 Year of Warranty, 06 Years of CAMC and additional 03 Years of CAMC (if extended by AAI).

7.8.2. During the currency of the Contract, the system must be scalable to support –

a. Changes to Hardware Models by the OEM including replacement of existing devices with newer models.
b. Changes to the Facial Matching Algorithms
c. Multiple biometric matching algorithms within the same central solution for a given biometric modality.
d. Changes in relevant rules, regulations, law of the land etc. which may lead to systemic changes; with or without change requests, as decided by AAI on a case to case basis.

8. Tentative Project Tenure

8.1. The End-to-End Solution Development, including System Requirement Finalization, Design, Development, Testing, Implementation on Cloud Platform, Commissioning and any other required process; must be completed within a period of 04 (Four) to 06 (Six) Months from the Date of Commencement of Work.

8.2. Additional 02 (Two) Months shall be allowed for Stabilization of Solution, Project Audits and Certifications.

8.3. Initial Site Survey for finalization of requited Hardware and Infrastructure must be completed within 02 (Two) Month from Date of Commencement of Work.

8.4. All required delivery and installation of required Hardware must be completed within 03 (Three) Months from Date of Issuance of Delivery Clearance.

8.5. All required Infrastructure Setup at any particular Airport must be completed within 03 (Three) Months from the Date of Issuance of first Delivery Clearance for that particular airport.

8.6. The overall time for Go-Live of the Solution at the initial set of 44 AAI Airports mentioned under Worksites shall be decided mutually by AAI and the Contractor, which shall not be more than 18 Months.

8.7. 1 Year Warranty shall be applicable from date of Go-Live of the Project.

8.8. 6 Years CAMC shall be applicable post completion of Warranty Period.

8.9. At its sole discretion, AAI may extend the CAMC for another 3 Years, based on satisfactory performance by the Contractor.

Annexure – I: Tentative Hardware Specification

A. Technical Specification for ASG/CISF Tablet with Stand

a. Make

b. Model

S. No.	Minimum Technical Specifications Required	Compliance (Yes/No)
1.	Industry grade tablet comprising of Minimum 10-inch touch screen, Full HD Resolution (600x1024) or better, Quadcore (Intel / Qualcomm / equivalent) processor or better, 128 GB SSD, 8.0 Megapixel rear-facing camera, 2.0 Megapixel front-facing camera. Provision of Android (version N-1) or above/ Windows (version N-1) or above with all future updates/ upgrades, where version N represents latest stable version in the market.	
2.	OEM Certified to tolerate extreme temperatures, humidity, rain, and other harsh environmental elements (MIL-STD-810H or equivalent).	
3.	The device must be provisioned with Secure Mobile Dock with key lock provides data and device safety, port replication, crash safety, and battery charger.	
4.	It must have flexibility to be mounted on floor stand, as per airport operational requirement. Any assembly/ sub-assembly for such mounting/ docking to be provisioned, all inclusive.	
5.	Battery life should be at least 4000mAH	
6.	Basic Connectivity Features i.e. Bluetooth, LAN, USB and Wi-Fi	
7.	ASG/CISF Tablet Accessories i.e. USB Cable, OTG Cable, Charger, Tempered Glass, Compatible Carry Case, Compatible Protective Cover, Compatible Earphones, Tablet Mount Stand, Handle/shoulder strap with Pen, Screen Protector**.**	
8	ASG/CISF tablet stand should have Height Adjustable capability.	
9	ASG/CISF tablet stand should have capability for 360 rotation.	

B. Technical Specification for Barcode Scanner with Stand

a. Make

b. Model

S. No.	Minimum Technical Specifications Required	Compliance (Yes/No)
1.	The Barcode Scanner must conform to IATA 792 Standards. All major 2D symbologies, including PDF417, QR Code, Data Matrix, AZTEC, CSC, Maxi code, Micro QR, Micro PDF417, GM, Code One on both paper & electronic screens.	

2.	Basic Connectivity Features i.e. Bluetooth, LAN & Wi-Fi along with USB port(s).	
3.	Must comply to RoHS Standards.	
4.	It must have flexibility to be either mounted on floor stand/ mobile as per airport operational requirement. Any assembly/ sub-assembly for such mounting/ docking to be provisioned, all inclusive.	
5.	Required Accessories i.e. USB Cable, OTG Cable, Tempered Glass, Compatible Protective Cover, Mount Stand, Screen Protector to be provisioned, all inclusive.	
6.	It must have flexibility to be mounted on floor stand, as per airport operational requirement. Any assembly/ sub-assembly for such mounting/ docking to be provisioned, all inclusive.	
7.	Scanner stand should have Height Adjustable capability.	
8.	Scanner tablet stand should have capability for 360 rotation.	

Annexure – II: Sample Components of IATA 792 Standard

	New item number	Element Description	Size	Repeated
Mandatory Items	1	Format Code	1	U
	5	Number of Legs Encoded	1	U
	11	Passenger Name	20	U
	253	Electronic Ticket Indicator	1	U
	7	Operating Carrier PNR Code	7	R
	26	From City Airport Code	3	R
	38	To City Airport Code	3	R
	42	Operating Carrier Designator	3	R
	43	Flight Number	5	R
	46	Date of Flight (Julian Date)	3	R
	71	Compartment Code	1	R
	104	Seat Number	4	R
	107	Check-in Sequence Number	5	R
	113	Passenger Status	1	R
	6	Field Size of variable size field	2	R
Conditional items - Flight segment # 1	8	Beginning of version number	1	U
	9	Version Number	1	U
	10	Filed Size of following structured	2	U
	15	Passenger Description	1	U
	12	Source of Check-in	1	U
	14	Source of Boarding Pass issuance	1	U
	22	Date of Issue of Boarding Pass (Julian	4	U
	16	Document Type	1	U
	21	Airline Designator of boarding pass	3	U
	23	Baggage Tag License Plate Number (s)	13	U
	31	1st Non-Consecutive Baggage Tag	13	U
	32	2nd Non-Consecutive Baggage Tag	13	U
	17	Field Size of following structured	2	R
	142	Airline Numeric Code	3	R
	143	Document Form/Serial Number	10	R
	18	Selectee indicator	1	R
	108	International Document Verification	1	R
	19	Marketing carrier designator	3	R
	20	Frequent Flyer Airline Designator	3	R
	236	Frequent Flyer Number	16	R
	89	ID/AD Indicator	1	R
	118	Free Baggage Allowance	3	R
	254	Fast Track	1	R
	4	For Individual airline use	Var	R
Security	25	Beginning of Security Data	1	U
	28	Type of Security Data	1	U
	29	Length of Security Data	2	U
	30	Security Data	100	U

PAGE LEFT BLANK

Annexure – III: Budgetary Quote Submission Format

(To be provided on Prospective Bidder's Letterhead)

Sl. No.	Item Description	Qty	Units	UNIT RATE (Exclusive of GST) (In INR)	Total Cost (Exclusive of GST) (in INR)
A	B	C	D	E	F = C*E
1	**Sub-Head 1: Implementation of Central Travel Document Authentication (CTDA) Application - One Time**				
1.01	End-to-End Development/ Deployment of AAI Travel Document Authentication (TDA) Core Application on Cloud including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	1	Lot		
1.02	End-to-End Development/ Deployment of Passenger Travel Validation Middle Layer on Cloud including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	1	Lot		
1.03	End-to-End Development/ Deployment of Travel Document Authentication (TDA) Orchestration Layer including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	1	Lot		
1.04	Integration and Networking between all operational Airlines DCS and Passenger Travel Validation Middle Layer including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	1	Lot		
1.05	End-to-End Development/ Deployment of Dashboard & Reporting Layer on Cloud including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	1	Lot		
2	**Sub-Head 2: Enablement of Designated AAI Airports - each airport basis**				
2.01	Local Airport infrastructure setup at Airports, including SITC of required network infrastructure, OFC cabling & provision of dedicated dual network link with CTDA Application including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	44	Lot		
2.02	Airport specific integration on cloud environment (including incremental provisioning) with CTDA Application including UAT, Production Go-Live and 1- Year Warranty from Date of Go-Live	44	Lot		
3	**Sub-Head 3: SITC of ASG/CISF Tablet and Scanners- each touchpoint basis**				
3.01	Supply of ASG/ CISF Tablets and required mounting provision with 1-year warranty from Date of Go-Live/ Commissioning.	250	Nos		
3.02	Provisioning of Client license(s) of ASG/ CISF Tablets, as required for the Project, with prior written approval of AAI	250	Lot		
3.03	Integration of ASG/ CISF Tablets, including Firmware integration, with CTDA Application, including 1-year warranty from Date of Go-Live/ Commissioning.	250	Lot		
3.04	Installation, Testing and Commissioning of ASG/ CISF Tablets including all required provisions for operationalization, such as electrical cabling from DB, LAN cabling from access switch, provision of UPS, cost of	250	Lot		

Sl. No.	Item Description	Qty	Units	UNIT RATE (Exclusive of GST) (In INR)	Total Cost (Exclusive of GST) (in INR)
A	B	C	D	E	F = C*E
	physical storage of device at site etc. (as required), system Configuration, Testing, UAT and Go-Live.				
4	**Sub-Head 4: SITC of Independent Barcode Scanner - each touchpoint basis**				
4.01	Supply of Independent Barcode Scanners and required mounting provision with 1-year warranty from Date of Go-Live/ Commissioning.	250	Lot		
4.02	Provisioning of Client license(s) of Independent Barcode Scanners, as required for the Project, with prior written approval of AAI	250	Lot		
4.03	Integration of Independent Barcode Scanners, including Firmware integration, with CTDA Application, including 1-year warranty from Date of Go-Live/ Commissioning.	250	Lot		
4.04	Installation, Testing and Commissioning of Independent Barcode Scanners including all required provisions for operationalization, such as electrical cabling from DB, LAN cabling from access switch, provision of UPS, cost of physical storage of device at site etc. (as required) , system Configuration, Testing, UAT and Go-Live.	250	Lot		
5	**Sub-Head 5: Other CAPEX Items**				
5.01	Rates for managing Change Request	10,000	Person Days		
5.02	External System Integration, which is not a part of current scope	1	Lot		
6	**1st Year of CAMC**				
6.01	1st Year CAMC for CTDA Application (Sub-Head 1), all inclusive	1	Lot		
6.02	1st Year CAMC for Enablement of Designated AAI Airports (Sub-Head 2), all inclusive, each airport basis	44	Lot		
6.03	1st Year CAMC for ASG/ CISF Tablets (Sub-Head 3), all inclusive, each touchpoint basis	250	Nos.		
6.04	1st Year CAMC for Independent Barcode Scanners (Sub-Head 4), all inclusive, each touchpoint basis'	250	Nos.		
7	**2nd Year of CAMC**				
7.01	2nd Year CAMC for CTDA Application (Sub-Head 1), all inclusive	1	Lot		
7.02	2nd Year CAMC for Enablement of Designated AAI Airports (Sub-Head 2), all inclusive, each airport basis	44	Lot		
7.03	2nd Year CAMC for ASG/ CISF Tablets (Sub-Head 3), all inclusive, each touchpoint basis	250	Nos.		
7.04	2nd Year CAMC for Independent Barcode Scanners (Sub-Head 4), all inclusive, each touchpoint basis'.	250	Nos.		
8	**3rd Year of CAMC**				
8.01	3rd Year CAMC for CTDA Application (Sub-Head 1), all inclusive	1	Lot		

Sl. No.	Item Description	Qty	Units	UNIT RATE (Exclusive of GST) (In INR)	Total Cost (Exclusive of GST) (in INR)
A	B	C	D	E	F = C*E
8.02	3rd Year CAMC for Enablement of Designated AAI Airports (Sub-Head 2), all inclusive, each airport basis	44	Lot		
8.03	3rd Year CAMC for ASG/ CISF Tablets (Sub-Head 3), all inclusive, each touchpoint basis	250	Nos.		
8.04	3rd Year CAMC for Independent Barcode Scanners (Sub-Head 4), all inclusive, each touchpoint basis'	250	Nos.		
9	**4th Year of CAMC**				
9.01	4th Year CAMC for CTDA Application (Sub-Head 1), all inclusive	1	Lot		
9.02	4th Year CAMC for Enablement of Designated AAI Airports (Sub-Head 2), all inclusive, each airport basis	44	Lot		
9.03	4th Year CAMC for ASG/ CISF Tablets (Sub-Head 3), all inclusive, each touchpoint basis	250	Nos.		
9.04	4th Year CAMC for Independent Barcode Scanners (Sub-Head 4), all inclusive, each touchpoint basis'	250	Nos.		
10	**5th Year of CAMC**				
10.01	5th Year CAMC for CTDA Application (Sub-Head 1), all inclusive	1	Lot		
10.02	5th Year CAMC for Enablement of Designated AAI Airports (Sub-Head 2), all inclusive, each airport basis	44	Lot		
10.03	5th Year CAMC for ASG/ CISF Tablets (Sub-Head 3), all inclusive, each touchpoint basis	250	Nos.		
10.04	5th Year CAMC for Independent Barcode Scanners (Sub-Head 4), all inclusive, each touchpoint basis'	250	Nos.		
11	**6th Year of CAMC**				
11.01	6th Year CAMC for CTDA Application (Sub-Head 1), all inclusive	1	Lot		
11.02	6th Year CAMC for Enablement of Designated AAI Airports (Sub-Head 2), all inclusive, each airport basis	44	Lot		
11.03	6th Year CAMC for ASG/ CISF Tablets (Sub-Head 3), all inclusive, each touchpoint basis	250	Nos.		
11.04	6th Year CAMC for Independent Barcode Scanners (Sub-Head 4), all inclusive, each touchpoint basis'	250	Nos.		
				Total Cost (in INR), exclusive of GST	
				GST @ 18%	
				Total Cost (in INR), inclusive of GST	