Request for Proposal

Selection of System Integrator for Enhancement, Operation, and Maintenance Support of Aadhaar Authentication Framework Govt. of Odisha

RFP Ref No. OCAC-NEGP-UIDAI-0001-2022-23022

Vol-II	Terms of Reference

ODISHA COMPUTER APPLICATION CENTRE
[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]
OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India
W: www.ocac.in | **T**: 0674-2567295/2567283 | **F**: 0674-2567842

Table of Contents

Abbreviations

APB	Aadhaar Payment Bridge
API	Application programming interface
ASA	Authentication Service Agency
ASP	Application Service Providers
AUA	Authentication User Agency
BCP	Business Continuity Planning
B.E.	Bachelor of Engineering
B. Tech.	Bachelor of Technology
BOM	Bill of Material
BSKY	Biju Swasthya Kalyan Yojana
CA	Certification Authority
CDAC	Centre for Development of Advanced Computing
CERTIN	Indian Computer Emergency Response Team
CIDR	Central Identity Data Repository
CMM	Capability Maturity Model
CSC	Common Services Centers
DBA	Data Base Architect
DBT	Direct Benefit Transfer
DeiTY	Department of Electronics and Information Technology
DR	Disaster Recovery
DTI	Directorate of Treasury and Inspection
e-KYC	Electronic Know Your Customer
FAQ	Frequently asked question
FIR	Fingerprint Image Record
FMR	Fingerprint Minutiae Record
FRS	Functional Requirement Study
GIGW	Guidelines for Indian Government Websites
HLD	High Level Design
HSM	Hardware Security Modules
HTTPS	Hypertext Transfer Protocol Secure
H/w	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IIN	Issuer Identification Number
IOS	iPhone Operating System
IRIS	Integrated Records Information System
ISO	International Organization for Standardization

IT	Information Technologies
KALIA	Krushak Assistance for Livelihood and Income Augmentation
KSA	e-KYC Service Agency
KUA	Know User Agency
KYR	Know Your Resident
MCA	Master of Computer Application
MIS	Management Information Systems
MSK	Mo Seva Kendra
NPCI	National Payments Corporation of India
OCAC	Odisha Computer Application Centre
OSDC	Odisha State Data Centre
OTP	One-Time-PIN
PID	Proportional, Integral, Derivative
PMP	Project Management Professional
PMU	Project Management Unit
QGR	Quarterly Guaranteed Revenue
RFP	Request for Proposal
SC&ST	Scheduled Caste (SC) and Scheduled Tribes (ST)
SLA	Service-Level Agreement
S/w	Software
SPV	Special Purpose Vehicle
SRS	System Requirement Specifications
SSL	Secure Sockets Layer
SSP	Software Solution Provider
UAT	User Acceptance Test
UIDAI	Unique Identification Authority of India
URL	Uniform Resource Locator
XML	Extensible Mark-up Language

1 Background

Odisha Aadhaar Authentication Framework is a centralized, secure & single source of information on state residents and is integrated with various departmental applications for the purpose of availing Government Welfare Scheme benefits. Aadhaar Authentication Framework is a repository of UIDAI data of residents, along with their demographic data and photograph. The biometric details like iris and fingerprints are not stored at the state level and are available with the UIDAI CIDR only. This helps the state government in maintaining a lean database, and ensures privacy of data.

To manage the state level data in a secured manner, Odisha Computer Application Centre (OCAC), the Technical Directorate of Electronics & Information Technology Department, Government of Odisha, implemented a comprehensive portal with basic software utilities for enabling seeding and authentication through Central Identity Data Repository (CIDR). This was started in the year of 2016.

The major objectives of Aadhaar Authentication Framework application are mentioned below –

a) Manage complete state level resident data in a digitized, centralized and secure manner
b) Enhance Aadhaar Data Security
c) Leverage Resident Data in Service Delivery Applications

Year	***Activities***
2016-2020	The web portal and mobile application has been linked to various departments to authenticate at the service delivery point through Aadhaar enable security system by integration with Aadhaar Authentication Framework of Odisha. The existing Aadhaar Authentication Framework portal has following modules: a) Authenticate Services b) eKYC validation c) Mobile Application d) MIS reports and Dashboard e) Web Service Integration f) Helpdesk

Year	*Activities*
2020	Aadhaar Data Vault has been introduced for generation of reference keys to reduce the risk of unauthorized access. This results in reducing the frequent usage of Aadhaar number. The application also prevents threats with respect to data leakage and made the Aadhaar ecosystem more secure and robust.
2022	Apart from Aadhaar Authentication Framework (with Aadhaar Data Vault), State DBT Portal has been on-boarded as one of the module.

d) Aadhaar authentication during delivery of citizen centric services

The sequence of implementation of Aadhaar Authentication Framework for last 05 years is given below:

2 Stakeholders Involvement

Primary Stakeholders

a) OCAC (as AUA)

b) All State Government Departments (as SUB-AUA)

c) UIDAI

d) MasterCard (as ASA)

e) BSNL (as ASA)

Secondary Stakeholders

a) Citizen

b) Employees

3 Existing Framework

The existing Aadhaar Authentication Framework portal, a single centralized platform provides the citizen of Odisha with a distinct digital identity and unique profile. This is helping the department authority to map all the services which the citizens are entitled for. It also allows the departmental officials to track the daily authentication status, success / failure transaction on a day to day process. Following modules / functions are already developed, implemented in the existing portal & continuing successfully since 2016.

Authentication	Enable Aadhaar-holders to prove their identity while availing government service. Also have provision for the service

Service	providers to confirm the resident's identity in order to provide services and give access to benefits. — It supports following type of authentication. • Biometric Matching (Finger Print Authentication , Iris Authentication) • Demographic Matching • One-Time-PIN (OTP) • Bulk Authentication of Data
E-KYC	— Provides an authenticated instant verification of identity that significantly reduce the time and cost of physical verification. — The e-KYC service Captures • Aadhaar number + biometric/OTP and forms the encrypted PID block. • KUA forms the Auth XML using the PID block, signs it, uses that to form final e-KYC input XML and sends to KSA. • KSA forwards the KYC XML to Aadhaar e-KYC service. • Aadhaar KYC service authenticates the resident and if successful responds with digitally signed and encrypted XML. • eKYC response (containing demographic data and photograph), by default, is encrypted with KUA public key. • KSA sends the response back to KUA enabling paperless electronic KYC.
MIS Reports and Dashboard	The web portal is generating audit trail report such as — Login Audit Trail — Authentication Audit Trail — Search Audit Trail — Service Audit Trail

Mobile Application	The existing mobile application was developed in Android Platform having following feature. — Mapping of different department services with the mobile application — Capturing image of Aadhaar card — Capturing beneficiary photo — Capturing information of the beneficiary — Validation of beneficiary details with the Aadhaar number or Enrolment Number
Aadhaar Data Vault (ADV)	— Store Aadhaar numbers collected by the AUAs/KUAs/Sub-AUAs — Reference Key generation — Generation of Vault storage report — Bulk Aadhaar Upload — Scheme monitoring
DBT Portal	— discussing on integration process and modalities with the software implementation agency who will integrate in the application with Aadhaar Authentication Framework — guiding the process of authentication on different technical requirements — Providing functionalities of the pre-production AUA service URL and guide the process of implementation — End to end integration support and giving the solution if any error occurs during integration — Management of integration with DBT Bharat Portal

3.1 Web Service Integration

The existing application has web service integration process that helped the departmental users to perform search operation in their existing application without logging in to the Aadhaar Authentication Framework application. The existing applications is used by various state departments and integrated with following services.

Integration Component	Owner Department	Purpose
Ration Card (PDS)	Food Supply and Consumer Welfare Department	Beneficiary Identification with Authentication
BSKY	State Health Assurance Society, Health & Family welfare Department	
Scholarship	SC&ST Development Department, Labour and ESI Department, Higher Education Department, School and Mass Education Department and Skill Development and Technical Education Department	
Housing Allotment	Housing & Urban Development Department	
ARPAN (Pension Revision Application) and Life Certificate	Finance Department	
Paddy Procurement	Food Supply and Consumer Welfare Department	
Mamata	Women and Child Development	
Land Registration	Revenue and Disaster Management Department	Registration with Authentication
Farmer Registration	Agriculture and Farmer's Empowerment Department	
ARPANA	Directorate of Treasury and Inspection	
Sugam Portal	Fisheries & Animal Resource Development Department and Agriculture and Farmer's Empowerment Department	
KALIA	Agriculture Department	

3.2 Technology Stack

The existing application has been developed by using following technologies: and hosted in Odisha State Data Centre (OSDC).

3.2.1 Web App

Operating System	Windows / LINUX
Platform	jdk 1.8, Spring Boot, Hibernate
DB Software	MySQL 5.7
Web Server	Jboss 7.0, Apache Tomcat 9.0

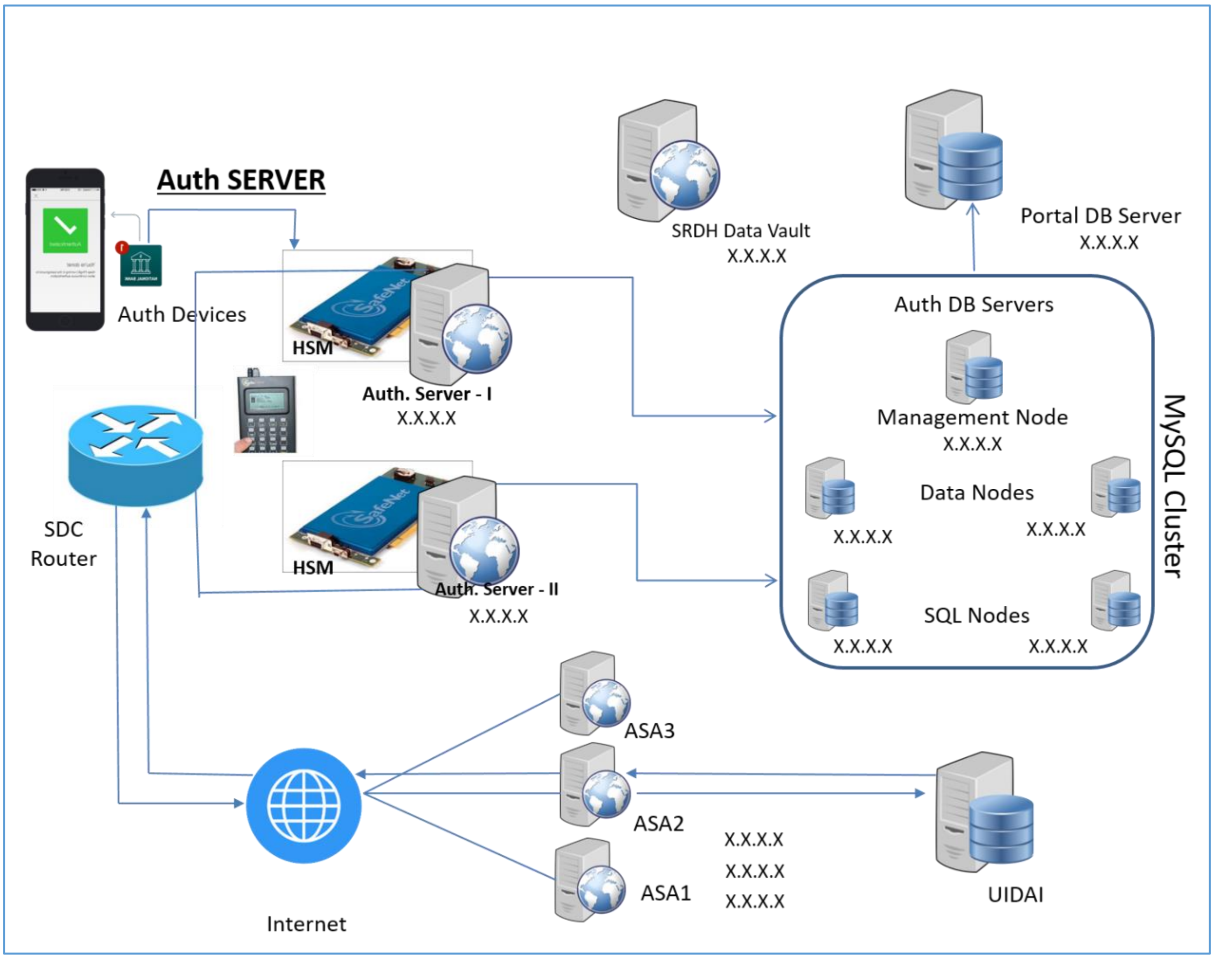
3.2.2 Mobile App

Operating System	Android
Platform	Native Android, Java, Android Studio
DB Software	Sqlite3
Web API	SOAP API, Restful API

3.2.3 DBT Portal

Operating System	Windows / LINUX
Platform	PHP 7.4
DB Software	MySQL 5.7
Web Server	Apache 2.0

3.3 Deployment Architecture



4 Scope of Work

4.1 Objective

Over the last few years, UIDAI has come up with new guidelines for effective authentication of Aadhaar keeping data privacy into consideration. The project is expected to improve the service delivery mechanism for residents in the state of Odisha as per the guidelines issued by UIDAI. Hence the existing Aadhaar Authentication Framework application needs to be enhanced to meet the following objectives

a) To enhance statistical analysis & achieve targeted delivery of welfare services
b) Provide Offline Aadhaar Verification facility
c) Digitally sign documents to authenticate the documents
d) Enable face authentication for beneficiaries in Mobile App for availing any state Government services
e) DBT Portal data sharing and reporting

f) Inspect and Analyze any fraudulent activities
g) Scheme on-boarding and authentication framework
h) ASA service management
i) Aadhaar Data Vault enhancements
j) Development of FIR service as per UIDAI guidelines
k) Application maintenance of existing Aadhaar Authentication Framework
l) Supply, installation and commission of new HSM as per the specification
m) Development and implementation of new module for Aadhaar Enrolment and related work for OCAC Registrar
n) Bulk Aadhaar verification as and when required by different departments/organisations
o) Aadhaar lookup and account validation of the scheme database as and when required through the NPCI mapper tool.
p) Compliance of Aadhaar Act/Notifications/memorandums issued by UIDAI time to time
q) Audit of Aadhaar Authentication Framework through any Cert-in empaneled firm as per latest Requesting Entity Compliance Checklist issued by UIDAI every year.

The Duration of engagement of System Integrator 5 years and six months from effective date of contract. 6 months of Development (Enhancement) as well as migration period and 5 years operation and maintenance support from the date of Go-live,

4.2 Overview

a) Complete takeover and management of the existing applications / databases in as-is condition from OCAC or by its nominated agency/team, along with all developments, enhancements, source codes, user manuals, system documents, design documents, integrations, infrastructure at OSDC till moving application to the new environment.
b) Technology upgradation of the existing modules
c) Study, development and implementation of new application modules / functions as per the requirement of this RFP
d) Application Maintenance Support of the new version of the application portal after its go-live.
e) API based integration such as third-party application/utility

f) Set-up and operation of technical support unit which shall provide technical and functional support at both onsite/offsite as specified in this document.

4.3 Proposed Technology up-gradation

The technology stack of existing Aadhaar Authentication Framework application shall be upgraded to the latest technology by the SI, as mentioned below table.

4.3.1 Web App

Technology	*Existing*	*Proposed Technology*
Operating System	Windows / LINUX	Windows / LINUX
Platform	jdk 1.8, Spring Boot, Hibernate	Jdk 11.0, Spring Boot, Hibernate
DB Software	MySQL 5.7	Oracle Database Enterprise (in Oracle ExaCC)
Web Server	Jboss 7.0, Apache Tomcat 9.0	Jboss 7.0, Apache Tomcat 9.0

4.3.2 DBT Portal

Technology	*Existing*	*Proposed Technology*
Operating System	Windows / LINUX	Windows / LINUX
Platform	PHP 7.4	PHP 8.0.
DB Software	MySQL 5.7	Oracle Database Enterprise (in Oracle ExaCC)
Web Server	Apache 2.0	Apache 2.4

4.4 Requirement Study

4.4.1 Prerequisites

The SI to follow and ensure following prerequisites before the requirement study

a) Consultation meeting with OCAC team

b) Identify and engage subject matter expert(s) as per the need

c) Readiness with the industry standard template for FRS and SRS documents

d) Readiness with the project traceability matrix template

4.4.2 Understand the Existing Applications / Databases

The SI will perform all the functions and services necessary to accomplish the transition of the entire knowledgebase, application, infrastructure and services under existing applications / databases from the present SI(s). The SI will be responsible for the overall management of the transition in accordance with the transition plan and will work to ensure the transition is completed on schedule and to identify and resolve any problems encountered. Further the SI will demonstrate its understanding of existing applications / databases and ability to support to reasonable satisfaction of OCAC, prior to the completion of Transition Phase, proving that it is ready to take over independently.

The responsibility of the SI during the phase includes following.

a) Submit a detailed Knowledge Transfer plan, listing all the activities from their end, including the expectations from the OCAC.
b) Preparation of a checklist to ensure proper knowledge transfer which will be reviewed and approved by OCAC.
c) OCAC will facilitate the training on existing applications / databases, operations manuals, procedure manuals, and source code control and deployment / installation guide.
d) Hands-on exposure to existing applications / databases would be facilitated by OCAC.
e) The SI shall assess and validate the existing IT assets and inventories related to this project and submit its report in the gap assessment report as per the project timeline.

4.4.3 New Modules

The SI shall perform a detailed functional and system requirement study from OCAC based on the new modules/functions proposed under functional requirement section in this document. Then the SI shall prepare the Functional Requirement Specification (FRS) and the System Requirement Specification (SRS) document and submit to OCAC for necessary action for its approval.

Following are the indicative list of enhancement to the made in existing application

- Introduction of face auth as per standard and procedure suggested by UIDAI which includes web application as well as mobile app.
- Improvement on existing Best Finger Detection (BFD) service

- Development of new module to provide bulk authentication service and Aadhaar Lookup service of NPCI for the Various Govt. Departments / Organisation along with tracking of request and services
- Enhancement of existing MIS module with following features
  - Service/Department/application wise transaction report
  - Minutes/month wise transaction report
  - Average response time success count report
  - Average response time error count report
  - Fluctuation report
  - Suspected Aadhaar report
  - Odd time transaction report
  - Blocking of suspected Aadhaar number
  - Various other types of analytical report after implementation of analytical tool
  - Sub-AUA on-boarding application processing module
  - Monthly unique transaction report
  - Any other report as per the requirement time to time

4.4.4 Development and implementation of module for Aadhaar Enrolment and related work

Apart from OCAC as AUA appointed by UIDAI for Aadhaar Authentication, OCAC is also appointed as State Registrar-cum-Enrolment Agency by UIDAI for Aadhaar enrolment of citizens of the state. Currently, OCAC is having about 2000 kits and every day average 1500 kits are active. In order to handle the Aadhaar enrolment, OCAC has engaged different system integrators for deployment of UIDAI certified operators at field level. The major responsibilities of these system integrators includes establishment of permanent enrolment centres at specified places, organizing special camps at schools, colleges, anganwadi centres etc. time to time as per the directions of OCAC. In order to handle the day today activities a software shall be developed with following functionalities

Enrolment hardware & software repository:

a) Provision to capture & maintain the “Enrolment hardware & software repository” / “Asset Register” for all the enrolment hardware, software procured by OCAC including certified biometric devices (for fingerprint and iris capture), used for capture of biometric data at the enrolling station.

b) Provision to update/import/export the "list/register" directly by uploading "Excel files".

Enrolment Centre (EC) and Enrolment Stations (ES):

a) Provision to capture & maintain the list of "Enrolment Centre (EC) and Enrolment Stations (ES).

b) Provision to update/import/export the "list/register" directly by uploading "Excel files".

c) Provision to maintain the "Contact Centre information" including the information pertaining to contacts at EC, Enrolment Centre address and working hours etc.

Operator boarding:

a) Provision to maintain the database of all "Operators and Supervisors" proposed to be deployed by the "Aadhaar System Integrators".

b) Provision to update/import/export the "Operators and Supervisors List" directly by uploading "Excel files".

c) Provision for Operator to submit his/her "On boarding Form" along with the required documents (with provision to upload documents in JPEG/PDF formats) to the Enrolment Agency/OCAC which in turn would be submitted to concerned "UIDAI Regional Offices" for verification.

d) Provision to reconcile the operator list after verification from the UIDAI Regional Offices.

e) Provision to capture/assign the "User Name" to operate the Enrolment Machine.

f) Provision to maintain a list of certified active operators/supervisors, requisite machines and hardware available to be deployed.

g) Provision to maintain a list of certified active operators/supervisors, requisite machines and hardware deployed in filed.

Knowledge Bank / Repository:

a) Provision to store & share the forms/procedures/masters including Pin Code Master/ list of valid documents/ utilities/ software's/ SFTP applications/ IEC guideline or documents/ etc.

Enrolment reconciliation & Payment reconciliation:

a) Provision for Operator to submit his/her "Explanation against the deficiency notice" along with the required documents (with provision to upload documents in JPEG/PDF formats) to the Enrolment Agency/OCAC which in turn would be submitted to concerned "UIDAI Regional Offices" for verification.

b) Provisions to calculate the successful enrolments/ deficiencies/ penalty based on the UIDAI's report. All the transactions during the previous month, irrespective of enrolment for new Aadhaar or update shall be analysed.

c) Provision to update/import/export the "reconciliation" directly by uploading "Excel files".

MIS:

a) Provision to generate various kind of MIS reports including the following:
   i. Enrolment hardware & software repository" / "Asset Register.
   ii. Enrolment Centre (EC) and Enrolment Stations (ES).
   iii. Operator Database.
   iv. Enrolment reconciliation report.
   v. Payment reconciliation report.

b) Provision to export generated reports to excel, PDF, Word, CSV etc.

c) Reports generated shall be in the printable format.

d) Provision to generate reports based on multiple filters viz; date/ enrolment category/ generation status/ etc..

4.4.5 Design

Prepare and submit updated detailed design & development plan as per the updated SRS considering the enhancement requirement. Design the solution architecture and specifications for meeting the requirements mentioned as part of this document including sizing of the required hardware.

4.4.6 Development

Identify, design and develop components / functionalities that are required to address proposed application requirements as mentioned in this RFP. Following documents shall be taken into consideration along with the developed components:

- Business process guides
- Data model descriptions
- Sample reports
- Frequently asked question (FAQ) guides
- Any other documentation required for usage of implemented solution

The SI shall implement a system for monitoring the SLAs and ensure that the system addresses all the SLA measurement requirements and calculation of applicable penalties as indicated in the document.

4.4.7 Integration

The system should support both push and pull of data to and from systems proposed to be integrated. It is required that a standard mechanism of data exchange should be built and implemented using an industry specified data exchange protocol through a secure channel. The SI will have to co-ordinate with the designated nodal agencies for integration and OCAC will facilitate this process. In addition, the solution should be designed in such a way that any future integration does not require any changes to the system.

4.4.8 Data Migration

The present database size would be approximately 1 TB. Data from the existing Aadhaar Authentication Framework to be migrated to the new framework. The data migration strategy and methodology to be prepared by the SI and submitted to OCAC for its approval before performing the data migration activities by the SI. The following activities will be carried out as part of the data migration:

a) Define all the specifications that are needed to populate the data into the new system

b) Prepare the data cleaning and migration plan and submit to concern authority for approval.

c) Prepare uniform codification of all data sets

d) Identification, configuration or development of the data upload / download programs for the Data Migration

e) Ensure minimum business downtime at the time of data cleaning and migration

f) Ensure the accuracy and completeness of the migrated data

g) Ensure migration of all data is completed by the time of go-live

h) Database of existing system would be migrated to the newly developed system.

i) The SI will be expected to understand the data which has been captured and devise a template so that meaningful information can be captured and entered into the new system

j) This template should have basic sanity check to prevent entry of incorrect information e.g. numerals should not be allowed in patient name etc.

k) It is the ultimate responsibility of the SI to ensure that all the datasets which are required for operationalization of the agreed user requirements are migrated.

l) OCAC will provide the database of the existing system and the SI is to manage the data extraction, normalization and migration for the new framework.
m) The SI should deploy a dedicated Oracle Database resource from M/s Oracle India or Oracle Consulting for period of 6 months.

4.4.9 Testing

a) Provide the testing strategy including Traceability Matrix, Test Cases and Conduct Testing of various components of the software developed / customized as per industry standards for Software Testing Life Cycle.

b) Details of the testing strategy and approach should be provided in the response.

c) Identify, inform regarding testing requirements along with its impacts and work in a manner to satisfy all the testing requirements by adhering to the testing strategy outlined.

d) Ensure deployment of necessary resources and tools during the testing phases and perform solution testing based on the approved test plan, document the results and fix the bugs found during the testing.

e) Make sure that the end product delivered meets all the requirements specified in the document.

f) Take remedial action based on outcome of the tests.

g) Provide complete support to the departmental officials or their representatives at the time of User Acceptance Testing (UAT).

h) Ensure that all issues raised during UAT are closed and signed-off from respective authority.

i) Ensure that each module & features developed under this RFP is tested as per the latest version of the IEEE 730 (Software Quality Assurance Processes) standards and comply with GIGW guideline.

4.4.10 Cyber Security Audit

a) The SI shall ensure that the solution is in compliance with the CERT-In Security Policy and Guidelines.

b) The SI shall appoint CERT-In empanelled auditor who shall be responsible for performing the security audit of the solution.

c) The cost of audit & rectification of non-compliances shall be borne by the SI

d) Carryout security audit before go-live of application and obtain the safe-to-host certification

e) Conduct periodic audit & certification as and when it is required as per the OSDC/Cloud policy.

f) The audit of Aadhaar Authentication Framework and related module should be carried out as per Requesting Entity Compliance Checklist/ other similar kind of document issued by UIDAI time to time and the State DBT Portal audit should be carried out as per OSWAP latest version.

g) The audit shall be performed at least on the below mentioned aspects.

- Accessibility Testing
- Application Security Audit
- Vulnerability Testing

h) The illustrative deliverables for this activity are mentioned below

Activity	***Responsibility***
First Round Audit Report	Auditor
Rectified solution and submission of next round of audit	SI
Next Round Audit Report	Auditor
If required, rectified solution & submission of next round of audit	SI
Compliance Confirmation	Auditor

4.4.11 Framework Security Audit as per UIDAI guidelines

Aadhaar Authentication Application Security Standard has been developed by UIDAI to assist system integrator engaged by requesting entities in developing authentication applications. The SI shall engage a Cert-IN empanelment vendor to audit of the Aadhaar Authentication Framework as per UIDAI shall be checklist once a year. Below Aadhaar authentication standard to be checked by system integrator for security compliances.

- Protect Aadhaar holder data
- Architecture, Design and Threat Modelling
- Authentication API compliance and Encryption
- Delivery of consent message for Aadhaar authentication within application
- Secure Network Communication

- Aadhaar Authentication Logs
- Application Logs
- Application Version Control
- Information Storage and Privacy
- Application Configuration Management
- Secure Application Development and Management
- Cryptography, Key Management and HSM

(latest version of Requesting Entity Compliance Checklist available at https://uidai.gov.in/images/resource/Requesting_Entity_Compliance_Checklist_V3.0.pdf)

4.4.12 SSL Certification

a) Secure connection between client and server through Secure protocol HTTPS

b) Encryption of Data during transmission from server to browser and vice versa

c) Encryption key assigned to it by Certification Authority (CA) in form of a Certificate.

d) SSL Security in the application server.

e) Bidder should quote for EV SSL for Aadhaar Authentication Framework (with related service) and DBT Portal

4.4.13 Training

a) Undertake training on a train to trainer mode.

b) Training would be done at State Headquarter in Bhubaneswar.

c) Set up the IT infra such as computer, network, LCD, etc. as required for providing the training in a successful manner.

d) Prepare training calendar and material for imparting training in consultation with OCAC and department officials.

e) Submit a hardcopy of the training material to OCAC before every training session.

f) In case of modifications, either in the training plans or substitutions of the regular trainers, proper communication with OCAC and Participating Department need to be made.

g) Conduct training (if required) on virtual mode and bear related expenditure for licensing (fixed & recurring).

h) OCAC will provide required classroom and IT infra for the class room training.

i) Training to the other users through virtual mode would be on need basis and the SI will bear related expenditure for virtual meeting licensing (fixed & recurring).

4.4.14 Online Help / Reference

a) It is proposed that the training contents / user manuals be made available to users in downloadable (PDF) format so that the users may refer / download it for their own personal reference as and when needed.

b) The downloadable training content should have proper indexing and internal references, mapped with key words, in order to allow any user to search and reach the desired content with the help of those key words.

c) It is envisaged that any user will be able to search and read the directions / information for the right content. On entering the key words for search criteria, the system should pull out and display the links to the content as mapped.

d) The system should support dynamic search facility i.e. as soon as the key words are changed; a new set of content links with page shall be displayed to the user.

e) Prepare Video & Audio based professional training material so that the users may refer it for their own personal reference as and when needed.

f) Availability of video & audio manual in the landing page of application in the form of YouTube link so that the end users can view it time & again.

4.4.15 Supply of tools and license

The SI shall procure tools and licenses for this project as per the specification and bill of quantity mentioned in this document vis-a-vis proposed in its technical proposal as part of the bid response. All the licenses will procured in the name of OCAC.

4.4.16 Deployment & Configuration

a) Deploy the application over the hardware infrastructure provided by the OSDC / Cloud.

b) Perform detailed assessment of envisaged solution requirements and assess the infrastructure requirements including Servers, Storage and Security, etc. for operationalization of the solution.

c) Responsible for end-to-end management of hosting and deployment of the application.

d) Responsible for configuration, installation and hosting of the application in High Availability mode at OSDC / Cloud.

e) Ensure deployment of the application as per the DR policy of OSDC/Cloud.

4.4.17 UAT & Go-Live

a) Preparation and submission of test strategy, test cases and test results.

b) Demonstration of module-wise functionalities/ features in staging environment.

c) Support designated authority for conducting the testing and provide access of the systems as required by them.

d) Rectification in the new application for any issues/ bugs/ and improvements/ Enhancements / up-gradations suggested Departments (if any) during the UAT without any additional cost.

e) After incorporation of the suggestion received during UAT the application will be declared as Go-Live.

4.4.18 Infrastructure Support

a) The existing solution is presently hosted in OSDC.

b) Post award of contract, it is expected the SI to provide detail hardware sizing for both production and staging instance. Based on sizing of the hardware, the additional hardware (if required) will be arranged/procured separately by OCAC.

c) Carry out the installation, maintenance & support of all the supplied software(s) on the newly procured / existing hardware for development, quality and production environment.

4.4.18.1 Implementing System Software & Tools

a) Design, implement/customize the solution and install supplies tools and licenses as mentioned in the BOM.

b) The observations of the audit shall be addressed and same shall be tested and verified again before go-live.

4.4.18.2 Business Continuity Planning

Currently, there is no Disaster Recovery (DR) or Business Continuity Plan (BCP) to address any disruption in implementation of the system. However, in future, if it is decided to go for DR / BCP, then the SI will suggest and support for an appropriate methodology in a cost-effective manner for this purpose. The IS shall share the DC, DR sizing and OCAC shall arrange necessary infrastructure in accordance to the sizing received.

4.4.18.3 Documentation

a) Undertake preparation of documents including that of infrastructure solution design and architecture, configuration files of the infrastructures, user manuals, Standard Operating Procedures, Information Security Management procedures as per acceptable standards.

b) Take sign-off on the deliverables (documents), including design documents, Standard Operating Procedures, Security Policy and Procedures from OCAC / OSDC Team and shall make necessary changes before submitting the final version of the documents.

4.4.19 Helpdesk Operation

The SI would be required to provide Helpdesk services for a period specified in this RFP to enable effective support to the internal and external users for operational and technical issues regarding the Aadhaar Authentication Framework. All the cost will be borne by the SI.

The helpdesk support will be available from 10 AM to 6 PM in all working days of Government of Odisha. OCAC will provide space and telephone for helpdesk. However, the SI has to provide required IT infrastructure to run the helpdesk.

The Service Provider shall provide at least the following services

a) Provision and supervision of personnel for the help-desk

b) Preferred language of communication mostly will be Odia

c) All calls will be assigned a ticket number and the number will be made available to the user

d) Helpdesk shall provide support for technical queries and other software / authentication related issues arising during day to day operations

e) The SI will adhere to the agreed service level with respect to the resolution of issues at various levels

f) All complaints/Queries / grievances of users will be maintained and followed up for resolution and an escalation matrix to be developed for any delay in resolution.

g) Resource engaged at Helpdesk also be assigned to coordinate with the different departments for Aadhaar integration and authentication related matters as and when required.

h) The SI must provide a web interface or integrate with existing "Janasunani" Portal for registration of queries/grievance by citizen.

The SI shall provide the following helpdesk performance monitoring reports.

a) Calls per week, month or other period;

b) Numeric and graphical representation of call volume;

c) Calls for each interaction tracked by type (calls for information on specific service, calls for specific enquiries, authentication related issues);

d) Any other reports as per requirement.

e) Service provider will submit monthly report on help desk operation to OCAC

Skill	**IT Helpdesk Executive**
Qualification & Experience	Graduate in any discipline with Minimum of 3 years' experience
Job Description	
– Resolve queries of all type of business users, register the query/ complaint in the application software, and take necessary action of Aadhaar Authentication Framework application. – Provide assistance in three languages i.e. English, Hindi & Odia. – Troubleshooting and resolving IT issues in a timely manner.	

Note: The resources will be deployed in the Sanjog Helpline Helpdesk, OCAC Tower to address the queries related to the application.

4.4.20 Subject Matter Expert

The SSP will engage this resource as full-time for this project and work in the SSP premises within the Bhubaneswar Municipality Corporation area. OCAC would have full rights to access the above resource for its supervision and call the resource when it is required, where the respective resource shall attend the queries and present at the premises within 1 hour. The skill and broad job description would be as per following.

<table>
<tr><th>Skill</th><th>Subject Matter Expert</th></tr>
<tr><td>Qualification & Experience</td><td>Post Graduate in any discipline with more than 15+ years' of experience in IT and Consulting filed</td></tr>
<tr><td colspan="2"><b>Job Description</b></td></tr>
<tr><td colspan="2">– Understanding on the Aadhaar Act and related notifications/memorandums issued by UIDAI time to time
– Understanding in the data protection bill
– Helping the line department during the on boarding to UIDAI framework
– Coordinating with department of solving Aadhaar related issues
– Consult OCAC on adhering the UIDAI policy by the SUB-AUAs
– Coordinating with UIDAI Regional Office and Headquarters for solving of various issues time to time
– Assisting OCAC and the scheme department during the UIDAI Audit
– Guide and Present the scheme department about the changes and its impact on UIDAI policy
– Educating higher level departmental officials on Aadhaar related compliances.
– Ensure the facts and details are correct so that the project's/program's deliverable(s) will meet the needs of the stakeholders, amendment, policies, standards, and best practices.
– Offers consulting services in managing business operations, also contributes to specialized knowledge, and provides mentorship to the line departments
– Before delivering the solutions to end-users, he/she ensures that the information has been represented accurately as per the subject expertise.
– Publicizing various important information and documenting processes to all stakeholders and board members
– Establish connect with key client stakeholders in the context of the opportunity and address concerns/needs.</td></tr>
</table>

- Ensure process guidelines are followed and met as documented & identify gaps in process compliance.
- Respond to queries raised by the team and provide appropriate feedback and analyze feedback received and error reports.

4.4.21 Application Support, Operation & Maintenance (O&M)

This section discusses the Application Support, Operations & Maintenance services to be provided by bidder with respect to Application Software & supporting IT Infrastructure Management (which is provided by bidder HSM as well as OSDC). However, server hardware maintenance is not scope of the bidder. OSDC shall share bare metal server/VM with required OS only. Any other required software/tool shall be provided by the bidder.

The selected bidder shall be required to provide operational and maintenance services for new System including all the connected software. An indicative list of activities and nature of support to be provided is mentioned below:

- Application Support & Maintenance
- System Administration and Trouble Shooting
- Co-ordination with Network Administration Team
- Database Administration and Trouble Shooting
- Application and System Software Administration (including performance tuning)
- Data backup and recovery as per the policy of OSDC.
- Application support and maintenance with enhancements as per requirement of Govt. of Odisha from time to time.
- Application and database level performance tuning

Bidder has to deploy the team with adequate manpower having expertise in database and application management & support for operation and management of entire application for a period of 5 year to carry out the above activities.

The bidder has to give details of methodology for Application Support, operation and management with team structure with proposed profiles in technical bid. The indicative activities are as follows

4.4.21.1 Application Support

a) Regular check-up of Complete Aadhaar architectures all components connections, connectivity and performance.

b) Instant action on any case of HSM (Hardware Security Module) Failure

c) Coordination with UIDAI team for technical issues and issue resolving.

d) Compliance audit of AUA-ASA application by UIDAI. Testing of new modules on staging servers before deployment.

e) Technical Support to Sub-AUAs in integration of Aadhaar APIs. Mapping of encryption and signing certificate with UIDAI.

f) AUA/ASA license key management (both production and Pre-production).

g) On-boarding of new Sub-AUAs in Aadhaar Ecosystem.

h) Biometric devices and UIDAI public certificate related help to end users.

i) Fraud Transaction Detection and taking necessary actions accordingly.

j) Management of complete fraud management system by using different fraud loggings

k) Execution of periodic Security Audit of application by OSDC.

l) Time to Time Application Updation as per Guidelines of UIDAI in all Auth APIs.

m) Optimization of the already developed reports

n) Tuning of transaction

o) User and access management

p) Application maintenance service should include State DBT Portal.

4.4.21.2 Software Maintenance

a) All patches and upgrades from OEMs (if any) shall be implemented by the I ensuring customization done in the solution as per the OCAC's requirements are applied

b) The SI shall provide unlimited support through Telephone / Email / Installation Visit as required as per the service window defined in this RFP

c) The SI shall address all the errors / bugs / gaps in the functionality in the solution implemented (vis-à-vis the FRS and SRS signed off) at no additional cost during the support phase.

d) Tuning of products / applications, databases, third party software's and any other components provided as part of the solution software including reconfiguration of the system in the event of any hardware/ network failures/ if any hardware/ network components have to be replaced, shall be the responsibility of the SI.

e) Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the SI and periodically submitted to OCAC.

f) Troubleshooting in HSM Integration with all components of application in case of failure of HSM device.

4.4.22 System/Infra Support

4.4.22.1 Database Administration

a) Regular monitoring & management of all the applications installed / re-installed and databases hosted as and when it required for the project

b) Installation & configurations the RDBMS software

c) Database administration, optimization and trouble Shooting

d) Database & file back-up as per the policy of OSDC/Cloud

e) Application Load balancing and Database Clustering

f) Perform Database, event & system log analysis

g) Key Infrastructure Management for Encryption/Decryption and Signing.

h) Coordination with OSDC team for network, connection, database and performance related issue and troubleshooting.

4.4.22.2 Server Administration

a) Installation, integration and commissioning new servers applicable for this project

b) Management & monitoring of severs such as Web, Application, Portal, Database & Middleware etc. in OSDC/Cloud

c) Configuration of server parameters, operating systems administration and tuning

d) Integration and user support on all supported servers, data storage systems, etc.

4.4.22.3 Security Administration

a) Regular analysis of events and logs generated

b) User ID and group management services

4.4.22.4 Backup & Restore Management

a) Preparation of backup plan

b) Backup of operating system, database and application as per OSDC/Cloud policy

c) Monitoring and enhancement of the performance of scheduled backups

4.4.22.5 System/Network Administration

a) Network configuration

b) Patch update

c) System Administration and Trouble Shooting

d) Application & System Software Administration (including performance tuning)

e) Application and database level performance tuning

f) Co-ordination with OSDC/Cloud Network Administration Team

4.4.23 Compliance Support

As per the agreement signed between OCAC and UIDAI, UIDAI shall have the right to levy Financial Disincentives on non-compliance of certain provisions/clauses under Aadhaar (Authentication) Regulations 2016 as well as agreement signed with UIDAI. Detailed list of the clauses is at Annexure-I.

The SI should provide necessary support to OCAC to monitor these provisions on regular basis. If required the SI should develop a tool for such monitoring and prepare a mechanism to monitor these provisions.

4.4.24 Project Management

The envisioned project is a multi-disciplinary initiative. An effective project management plan and commitment to adhere to it, is a mandatory requirement. The project plan should also include the resource, task and time plan for the entire duration of the project. The SI shall employ best practices in project management methodology to ensure that the envisioned project components are developed and implemented within the defined time period. A detailed project management plan shall be handed over to the department to keep track of the progress of the project.

4.4.25 Guiding Principles

The solution should adhere to the following principles.

4.4.25.1 Standards

a) The system architecture should be based on industry standards and protocols

b) The system shall be centrally deployed and globally accessed

c) The system shall be designed to be scalable and easily extensible

d) The system should be flexible to cater to changing business, industry and compliance requirements (including reporting requirements in proper formats)

4.4.25.2 Application

a) All applications must take into account appropriate security, performance, efficiency and maintainability issues.

b) The ownership of the product licenses would be with OCAC

c) Upgrade to new releases should not become mandatory for the next five years from the date of installation.

4.4.25.3 Integration

The integrated solution design should include framework for integration of both internal and external applications and services using suitable architecture.

4.4.25.4 Data

a) Data will be owned, shared, controlled and protected as a corporate asset of the OCAC.

b) Data should only be accessed through application / interfaces to create, update and delete. There should not be any direct access to the data layer for users.

4.4.26 Data Security

a) Provide strategy to maintain data security at the application level, database level, messaging and middleware level

b) Provide security strategies when the applications are accessed by the resources from outside the network

c) Provide strategies of encryption and security for external transaction with partner network and systems

4.4.27 Adherence to Standards

The system shall comply with relevant defined industry standards (their latest versions as on date) wherever applicable. This shall apply to all the aspects of solution including its design, development, security, installation, and testing. The suggested architecture must be scalable and flexible for modular expansion. It should ensure ease of integration with software / applications developed using common industry standards, since the solution may be linked and connected to other sources (websites, contents, portals, mobile app systems of other user departments etc.) as well as there may be loose/tight integration with backend system of other departments depending on individual service processes. The solution architecture should thus have provision to cater to the evolving requirements of the Department.

A reference list of the minimum industry standards which the system components should adhere to is mentioned below:

Component	***Standards***
Information Access / Transfer Protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open Standards
Portal Development	W3C Specifications
Document encryption	PKCS specification
Information Security	ISO 27001 certified System
Operation	ISO 9001 Certified
Service Management	ISO 20000 specifications or latest
Project Documentation	IEEE/ISO Specifications for documentation
Data Standards	All-important data entities should be in Line with standards published by DeiTY
Personal Data Protection/Data	IT Act 2000 and Aadhaar Act 2016

Component	*Standards*
Protection	

4.5 Security, Integrity & Confidentiality

a) **Web Services Security:** System shall comply with all the Web services including routing, management, publication, and discovery should be carried out in a secure manner. Those who are using the Web services should be able to utilize security services such as authentication, authorization, encryption and auditing. Encryption of data shall take place at client level itself. Application server shall provide SSL security.

b) **Data Integrity and Confidentiality***:* Data integrity techniques need to be deployed to ensure that information has not been altered, or modified during transmission without detection. Similarly, Data confidentiality features are also to be applied to ensure that the data is only accessible by the intended parties.

c) **Transactions and Communications:** With respect to the Data Transactions and Communications, system needs to ensure that the business process are done properly and the flow of operations are executed in correct manner.

d) ***Non Repudiation Security*****:** The application shall have the Non-repudiation security services to protect a party to a transaction against false denial of the occurrence of that transaction by another party. End-to-End Integrity and Confidentiality of Messages, integrity and confidentiality of messages must be ensured even in the presence of intermediaries.

e) ***Database Controls*****:** The database controls for online transaction processing systems like access to database directly, access to database through application, access to log files, access by the remote terminals, DBA controls, backup policy and backup procedures.

4.6 Change Request Management

Looking into the length of the project implementation period it is very usual to find changes in business logic frameworks. In such scenarios, there may be a need of modification of the software modules beyond FRS/SRS/Scope document. It may also be required to develop new software modules beyond the coverage of FRS/ SRS/ Scope document.

a) The activities that will be treated as enhancement services is mentioned below:

- Functional changes in the application
- Development of new module/sub-module/Form/Report in the developed system
- Changes in the workflow or core application framework
- Integration with any new system
- Additional onsite resources in the project

b) The procedure for executing the change request is as follows:

- Analysis: Analyses the changes suggested and submit an effort estimation including timeline to OCAC
- Approval**:** OCAC shall do the due diligence and provide approval on the effort and timeline suggested.
- Incorporation**:** After receiving the approval from OCAC, team will incorporate the changes in the application.
- On approval, deliver the services and raise the claim as per actual according to the Commercial Bid.

4.7 Exit Plan

a) Provide systematic exit plan and conduct proper knowledge transfer process to handover operations to OCAC technical team at least three months before project closure.

b) OCAC will work closely with the SI during knowledge transfer of testing, staging and production environment.

c) All knowledge transfer should be documented and possibly recorded.

d) Ensure capacity building of the IT resource persons of OCAC on maintenance of software and infrastructure.

4.8 Project Documentation

Below list of documents needs to be submitted to OCAC during the project contract period, as per the requirement of OCAC.

a) Latest version of Source Code

b) System Requirement Study Documents

c) System Design Document

d) Test Plans and Reports

e) Issue Logs

f) User Manual

g) Application Installation & Configuration Manual

h) API document

i) Report of Security Audit & Safe-to-Host Certificate

j) Any other documents defined under Timeline & Tentative Deliverables

k) All the above documentation should be done as per IEEE/ISO/CMM Standard

4.9 Expected Deployment of Personnel

a) The bidders shall furnish resumes of key personnel to be engaged during software study, design, development, testing, UAT, implementation, operation & maintenance phase.

b) The bidder shall submit a detailed work plan showcasing involvement of key resources in their technical proposal.

c) The bidder shall engage the same personnel for the period of at least six months from date or commencement of project.

d) The resources will work from the bidder's premises. However the resources should be available at client office for any meeting or discussions required by the client as per its convenient.

e) The minimum criteria for key resources are as follows.

Competency Area	Minimum Educational Qualification and Experience
Program Manager	– B.E/B.Tech/MCA & MBA – Minimum 20 years' experience of handling similar large projects in IT Sector. – Out of these, 10 years' experience in handling state wide rollout project Certification: Prince2 or PMP
Project Manager	– BE/B.Tech/MCA – Minimum 12 years' experience of handling similar large projects in IT Sector. – Out of these, 7 years in the field of software development and implementation. Out of these 7 years, 5 years' experience in healthcare domain for any government department in India. – Certification: Prince2 or PMP
Tech Lead	– BE/B.TECH/MCA

Competency Area	Minimum Educational Qualification and Experience
	– Minimum 9 years' experience in the field of software development and implementation. – Out of these 9 years, 4 years' experience in healthcare domain for any government department in India.
Solution Architect	– B.E/B. Tech/MCA – Minimum 10 years of experience in the field of software design & development – Out of these 10 years, At least 5 years' experience in large-scale software projects as a solution architect – Certification: TOGAF or relevant IT certification
Software Test Lead	– BE/ B.TECH/ MCA – Minimum 8 years' experience in software testing. – Certification: ISTQB
Database Administrator	– B.TECH / MCA – Minimum 6 years' experience in large scale software projects as DBA. – Certification: relevant OEM certification
Developer	– B.E/B. Tech/MCA/MSC(IT) – Minimum 5 years of experience in the field of software design & development using JAVA
Security Expert	– B.E/B. Tech/MCA – Minimum 5 years of experience in the field of data security – Relevant Information Security certification

4.10 Expected Project Timeline

Sl#	Milestone	Timeline
a)	Helpdesk Operation	Within 7-days form the date of contract
b)	Engagement of Subject Matter Expert	Within 7-days form the date of contract
c)	Handover & Takeover process	Within 2-months from the effective date of contract
d)	Handover / Takeover and Application Maintenance Support of the existing Aadhaar Authentication Framework	From the date of completion of Handover & Takeover process till go-live of the new version of the Aadhaar Authentication Framework

Sl#	Milestone	Timeline
e)	Submission of System Requirement Study document	Within 1-month from the effective date of contract
f)	Migration of database (from MY SQL to Oracle)	Within 2-months from the effective date of contract
g)	Deployment of OEM Resource (Database Administrator)	Within 1-month from the effective date of contract
h)	Completion of design and development of the new version of Aadhaar Authentication Framework	Within 4-months from the effective date of contract
i)	Completion of User Acceptance Test (UAT) of the new version of Aadhaar Authentication Framework	Within 5-months from the effective date of contract
j)	Cyber security audit certification, configuration & go-live the App	Within 6-months from the effective date of contract
k)	Supply and installation of Oracle License	Within 6-months from the effective date of contract or direction from OCAC whichever is earlier
l)	Supply and installation of Analytical Tool	Within 6-months from the effective date of contract or direction from OCAC whichever is earlier
m)	Supply and installation of HSM	Within 6-months from the effective date of contract or direction from OCAC whichever is earlier
n)	Application Maintenance Support of the new version of the Aadhaar Authentication Framework App	5-years from the date of go-live of the new version of the Aadhaar Authentication Framework App

4.11 OCAC Responsibilities

a) Assign a nodal officer who will be single point of contact from the beginning of the project till successful implementation.

b) Provide necessary support to the development team of the SI for smooth execution of project.

c) Provide all the relevant documents and information during the system study and analysis.

d) Facilitate the Software Solution Provider for the third party software integration.

e) Provide approval of SRS Document, User Acceptance Test certificate, Go-Live Certificate, approval of activity report during Operation & Maintenance Support phase, AMC etc.

f) Conduct exclusive hand-holding on the existing Aadhaar Authentication Framework to the SI. Following activities shall be taken into consideration during handover process:

   – Establish a transition team
   – Create a transition plan
   – Provide detailed documentation
   – Ensure multifaceted knowledge transfer
   – Get access to all third-party services
   – Transfer codebase ownership
   – Provide proper understanding on the source code, database table structure etc.

g) Provide hosting infrastructure in the Oracle ExaCC along with SMS and Email Gateway etc.

About IaaS and PaaS (ORACLE ExaCC)

OCAC has provisioned the ORACLE ExaCC of Quad Rack infrastructure at OSDC (Odisha State Data Centre) for different projects. Oracle ExaCC is the simplest and robust way to move an organization’s business-critical Oracle Database workloads to the On-premises or Cloud. It simultaneously runs Oracle ExaCC Database Service and the fully managed Oracle Autonomous Database Service inside customers’ data centres and behind their firewalls to help meet strict data residency and security requirements. Built using the latest ExaCC technology delivers the highest cloud database performance, scale, and availability, enabling organizations to run all types of database workloads faster. Now Oracle makes it easier and less expensive for customers to adopt Autonomous Database by running it on VMs in ExaCC.

Currently the infrastructure has been used by two major projects (BSKY and SPDP).
The configuration of environment is given below.

Features	Details	
Hardware Configuration	Physical Cores to run database – 120	80 Cores Available
	RAM (TB) - 2.5TB	1.5 TB Available
	Flash capacity (TB) - 70TB	40 TB Available
	Backup - 10TB	5 TB Available
	SQL Flash Read IOPS - 4.5 Mn	-

Features	Details	
	SQL Flash Write IOPS - 1.5 Mn	-
	Usable disk space - 190TB	150 TB Available
	Network - 4 x 10/25 Gb SFP28 (Fiber) Ethernet	-
Workload Types	The infrastructure is designed to handle the below type of ORACLE database platform – OLTP Cloud Data Warehouse – In-memory Analytics – In-database Machine Learning – Database Consolidation	
Placement	Odisha State Data Centre, OCAC	
Infra Management	The Infrastructure is managed by ORACLE Team	
Bandwidth & Latency	100Gbps active-active internal network fabric	
High Availability	Active-Active Mode	
Control Plane	Available	
Backup	Automatic built-in database backup facilities, with weekly full backups & daily incremental backups.	
Scalability	The solution shall be horizontally scalable.	

4.12 Performance Requirement (SLAs)

The purpose of this Service Level Agreement (herein after referred to as SLA) to clearly define the performance criteria that shall be adhered by the SI during the contract period.

Sl#	Major Area	Parameter	Requirements	Penalty
a)	Availability of application	Application covering all the features	98% availability round the clock and Computation will be done on monthly basis. Note : Fault at application level only	Up to 90-97.99% - 1% of application development cost. Less than 90%- 2% of application development cost

Sl#	Major Area	Parameter	Requirements	Penalty
b)	Resolution Time for Aadhaar Authentication Framework (Bug fixing)	Time taken by the Bidder to fix the problem	Within 6 hours of reporting	6hrs to 24 hrs @0.01% of application development cost. Beyond 24 hrs 0.1% of application development cost.
c)	Resolution Time for Authentication related issues	Time taken by the Bidder to fix the problem	Within 3 hours of reporting	3hrs to 6 hrs @0.01% of application development cost. Beyond 6 hrs 0.1% of application development cost.

Note: Penalty will be imposed on operation and maintenance support cost of respective QGR. Maximum ceiling of the penalty will be 10% cost of the operation and maintenance support of respective year.

4.13 Waiver of Penalty

If at any time during the contract, the selected SI should encounter conditions impending timely performance of service, the selected SI shall promptly notify to OCAC in writing of the fact of the delay and its likely duration along its cause(s). As soon as practicable after receipt of the selected SI's notice, OCAC shall evaluate the situation and may at its discretion waive the penalty on the request of the selected SI.

4.14 Bill of Material & Quantity

4.14.1 Software and Services

Sl#	Category	Items	Qty
a)	Handover / Takeover and Application Maintenance and Support of the existing Aadhaar Authentication Framework application	As per the scope mentioned under the relevant clause(s) of this document.	6 Months

Sl#	Category	Items	Qty
b)	Implementation of new version of the Aadhaar Authentication Framework	Study, design, development, security audit, training, go-live, documentations, etc. as per requirement mentioned under the relevant clause(s) of this document.	Lump Sum
c)	Development and implementation of software for Aadhaar Enrolment and related work	Study, design, development, security audit, training, go-live, documentations, etc. as per requirement mentioned under the relevant clause(s) of this document.	Lump Sum
d)	Application operation, Maintenance Support of the new version of the Aadhaar Authentication Framework	Application Operation Support, Software Maintenance, System Support, etc mentioned under the relevant clause(s) of this document.	5-years
e)	Cyber Security Audit of the complete application by CERT-IN empanelled agency/auditor (including DBT Portal)	As per the scope mentioned under the relevant clause(s) of this document.	10 times
f)	Security Audit of Aadhaar Framework by CERT-IN empanelled agency/auditor as per the UIDAI Guideline	As per the scope mentioned under the relevant clause(s) of this document.	5 times
g)	Helpdesk Operation	Helpdesk support as per scope mentioned under the relevant clause(s) of this document with flowing quantity IT Helpdesk Executive | 2	5.5 Years

Sl#	Category	Items	Qty
h)	Subject Matter Expert	As per scope mentioned under the relevant clause(s) of this document with flowing quantity Subject Matter Expert 1	5.5 Years
i)	SSL certificate	As per the scope mentioned under the relevant clause(s) of this document.	5-Years
j)	On boarding of new schemes	As per the scope mentioned under the relevant clause(s) of this document.	As per requirement

4.14.2 Infra and Services

Sl#	Category	Items	Qty
a)	Oracle Licenses (Perpetual)	As per the scope mentioned under the relevant clause(s) of this document.	8 Nos.
b)	Oracle Licenses (Perpetual) - Annual Technical Support	As per the scope mentioned under the relevant clause(s) of this document.	5-Years
c)	OEM Resource (Database Administrator) for DB migration and related activities thereof	As per the requirement mentioned under the relevant clause(s) of this document.	One resource for six months
d)	Analytical Tool	Supply of tools as per the scope mentioned under the relevant clause(s) of this document and quantity proposed by the SI	License with 5-year support
e)	HSM	Supply and Installation of HSM before UAT of Application as per the scope mentioned under the relevant clause(s) of this document.	2 Nos with 5-year support

Contract duration would be 5 year and 6 months from the effective date of contract. The contract period may be extended for another 2 years based on the requirement and performance of the SI. Further extensions (if required) may be done on mutual agreement between OCAC and SI.

4.15 Payment Terms

Sl#	Milestone	Deliverables	Payment Terms
a)	Handover / Takeover and Application Maintenance Support of the existing Aadhaar Authentication Framework App	Activity report	Quarterly payment of the cost
b)	Completion of system requirement study (SRS)	SRS document approve by OCAC	– 20% of implementation of new version of the Aadhaar Authentication Framework cost – 20% of cost against Aadhaar enrolment and related work
c)	Completion of User Acceptance Test (UAT)	UAT Certificate by OCAC	– 40% of implementation of new version of the Aadhaar Authentication Framework cost – 40% of cost against software for Aadhaar enrolment and related work
d)	Supply of HSM	Delivery challan duly signed by OCAC	90% of HSM cost
e)	Supply of Analytical Tool and license with 1st	Issue of license in the name of OCAC	90% of Analytical Tool cost

Sl#	Milestone	Deliverables	Payment Terms
	year Annual Technical Support)		
f)	Supply of Oracle license with 1st year Annual Technical Support)	Issue of license in the name of OCAC	90% of Oracle license cost
g)	Configuration and go-live the new version of Aadhaar Authentication Framework	Go-live certificate by OCAC	– 20% of implementation of new version of the Aadhaar Authentication Framework cost – 20% of cost against software for Aadhaar enrolment and related work – Balance 10% of HSM cost – Balance 10% of Analytical Tool cost – Balance 10% of Oracle License cost
h)	Application Maintenance Support of the new version of the Aadhaar Authentication Framework	Activity report	– 100% of Application Maintenance Support cost of the new version of Aadhaar Authentication Framework equally divided by duration (quarter) – Balance 20% of implementation cost of new version of the Aadhaar Authentication Framework equally divided in 4-quaters (first year)
i)	Helpdesk Operation	Activity report	100% of IT helpdesk cost equally divided by duration (quarter)

Sl#	Milestone	Deliverables	Payment Terms
j)	Subject Matter Expert	Activity report	100% of Subject Matter Expert cost equally divided by duration (quarter)
k)	New Scheme Onboarding	Acceptance certificate by OCAC	100% of on boarding of new schemes cost after successful on boarding of scheme
l)	Change Request Management	Acceptance certificate by OCAC	The payment shall be made only after change request activities are complete in all respect based on the man months used for the Change Request and certification by OCAC thereof
m)	Cyber Security Audit of the complete application	Submission of the certificate by the CERT-IN empanelled agency/auditor	100% of the Cyber Security Audit cost
n)	Security Audit of Aadhaar Framework	Submission of the certificate by the CERT-IN empanelled agency/auditor	100% of the Security Audit cost of Aadhaar Framework
o)	Configuration of SSL certificate and it’s renewal year on year	Submission of relevant documents	100% of the SSL cost
p)	Annual Technical Support of the supplied **tools and license** from 2nd year onwards	Documentary evidence on support of renewal	100% of the yearly quoted cost will be paid at the beginning of respective year
q)	OEM Resource (Database Administrator)	Activity report	100 % OEM Resource cost equally divided by duration (quarter)

4.15.1 Recurring Expenses

OCAC will provide SMS and e-Mail Gateway. However, if required, expenses incurred for SMS, Email would be reimbursed as per actual basis. So the SI will take prior approval from OCAC on the tentative requirement along with the estimate before purchase of these services.

4.16 General Conditions

a) Payment schedule - Payments to the SI after successful completion of the target milestones (including specified project deliverables), would be made as under: -

b) The supplier's/ selected SI's request for payment shall be made to the purchaser in writing, accompanied by invoices describing, as appropriate, the goods delivered and related services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.

c) Due payments shall be made promptly by the purchaser, generally within thirty (30) days after submission of an invoice or request for payment by the supplier/ selected SI/authorized partner, and the purchaser has accepted it.

d) The currency or currencies in which payments shall be made to the supplier/ selected SI under this Contract shall be Indian Rupees (INR) only.

e) All remittance charges will be borne by the supplier/ selected SI/authorized partner.

f) In case of disputed items, the disputed amount shall be withheld and will be paid only after settlement of the dispute.

g) Payment in case of those goods which need testing shall be made only when such tests have been carried out, test results received conforming to the prescribed specification.

h) Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this bidding document, will be deducted from the payments for the respective milestones.

i) Taxes, as applicable, will be deducted/ paid, as per the prevalent rules and regulations at the time of billing. Legitimate payment shall be made within 30 working days of the receipt of invoice along with supporting documents subject to penalties, if any.

5 Functional Requirements

5.1 Analytical Reports

5.1.1 Analytical Dashboard & MIS

The SI shall provide various analytical report on the data available in the Aadhaar Authentication Framework application.

Sl#	Functional Requirements
FR01	The analytical dashboard should enable the departmental officials to view dynamic report in tabular as well as graphical manner.
FR02	The analytical dashboard should have the capability to perform following type of analysis: a) Daily/Monthly Transaction b) Sub-AUA wise Transaction c) Error code wise analysis d) Device wise transaction analysis e) e-KYC transactions f) Failure Statistics g) ASA wise transaction h) Reference number generation statistics i) DBT Schemes Data
FR03	SI shall set up a reporting framework that would deliver reports across multiple file formats, dashboards and alerts to the business users.
FR04	OCAC should be given the ability to redefine report formats as needed and should enabled to filter, sort and drill down in to reports.

The proposed OEM tool shall cater to the below functionalities

Sl#	Functional Requirements
FR01	Provision to generate turnaround time wise report, scheme wise report
FR02	The solution should provide easy-to-use ad hoc query and analysis.
FR03	Users should be able to drill, pivot, and filter their data directly on a dashboard, while a rich set of prompts and powerful right-click interactions open up even more advanced analysis capabilities.

Sl#	Functional Requirements
FR04	Users should be able to see information filtered and personalized based on their identity, function, or role processed via predefined security rules.
FR05	The solution should offer a logical view of metrics, hierarchies, and calculations expressed as understandable concepts.
FR06	Users should be able to quickly and seamlessly transfer their data, layout, and format of a dashboard or analysis to an output or data export file.
FR07	The Analytics platform should provide a powerful, near-real-time, multistep alert engine that can trigger workflows based on business events and notify stakeholders via their preferred medium and channel.

5.2 Fraud analytics

In authentication various frauds that have been observed in the past and present times. Such frauds can be eliminated by fraud management system in the current Aadhaar system. SI has to develop or implement the tool to analyze and eliminate frauds.

Sl#	Functional Requirements
FR01	Management of complete fraud management system by using different fraud loggings
FR02	Fraud Transaction Detection and taking necessary actions accordingly
FR03	Eliminates or reduces redundant or inconsistent data
FR04	Stores all information pertinent to a fraud case, including detailed/comparison investigation information for further future access

5.3 DBT Portal data sharing and reporting

The purpose of this module shall provide an understanding of the respective schemes data exchange through State DBT Portal to the Electronics & Information Technology Department of Odisha on monthly basis. Following provisions shall be available in the solution:

Sl#	Functional Requirements
FR01	Provision to display DBT schemes of various Departments by fetching data from DBT portal
FR02	Shall part of the reform of the Public Service Delivery System
FR03	The solution should have provision to ensure faster flow of information to Primary stakeholders as well as Secondary stakeholders.
FR04	Provision for De-duplication and accurate targeting of the beneficiaries.
FR05	Provision for centralized authentication of Aadhar through Web API.
FR06	Data transfer into Aadhaar Authentication Framework Portal in real-time mode.
FR07	Faster generation of aggregated figures of each scheme, whether State/District wise.
FR08	Easier monitoring of complied Monthly Progress of schemes through Dashboard.

5.4 Aadhaar Offline e-KYC

Aadhaar paperless offline e-KYC shall have the below functionalities:

Sl#	Functional Requirements
FR01	The application shall eliminates the need for the resident to provide photo copy of Aadhaar letter and instead resident can download the KYC XML and provide the same to agencies wanted to have his/her KYC.
FR02	The XML file shall be password-protected for security reasons.
FR03	The system shall have the functionality to provide an authenticated instant verification of identity
FR04	System should provide Secure sharable document which shall be used by any Aadhaar number holder for offline verification of identification
FR05	Provision for Offline Aadhaar Verification facility to service providers/Offline Verification Seeking Entity (OVSE) without the need to collect or store Aadhaar number

5.5 e-Sign

Electronic signature service (eSign) shall enables Application Service Providers (ASP) to enable their users to electronically sign documents using Aadhaar to digitally sign a document within seconds from anywhere and anytime.

Application Service Providers (ASP) can integrate this service within their application to offer Aadhaar holders a way to sign electronic forms and documents.
Features of implementation of Aadhaar e-Sign shall be:

Sl#	Functional Requirements
FR01	System should have the functionality to e-Sign with Aadhaar of Aadhaar holder through an Aadhaar number or a linked phone/email
FR02	Shall have provision of ensuring records are authentic and legitimate
FR03	System shall have the functionality with the Aadhaar-based authentication. By using the application the users shall be benefitted from privacy and ease and is Eco-friendly with an electronic signature.

5.6 Aadhaar based face authentication mobile apps (Android)

The mobile application shall be developed in Android platform. The mobile app shall have below functionalities.

Sl#	Functional Requirements
FR01	Application should allow the verification of Aadhaar card holders anytime and at any place
FR02	Should capture live person’s face for Aadhaar authentication using Face Authentication Technology
FR03	Provision for Aadhaar authentication through iris and fingerprint scans
FR04	Shall have provision to re-register themselves for updating photographs/ face recognition by using OTP
FR05	Shall have the functionality to allow user to give consent and confirm the same for the further procedure
FR06	User shall have provision to click yes to approve for the ‘Face Scan’

5.7 System Integration

5.7.1 Integration with NPCI

Sl#	Functional Requirements
FR01	Shall have functionalities of getting mapped in NPCI mapper to the bank in which user has given the Aadhaar number at the last
FR02	Shall have functionalities of NPCI mapper using the latest IIN (Issuer Identification Number) of the bank in which the user has seeded their Aadhaar number to transfer benefits and subsidies registered with respective scheme in their bank account

The only inputs required for a beneficiary to do a transaction under this scenario are:-

a) Bank Name
b) Aadhaar Number
c) Fingerprint captured during enrolment

5.7.2 Aadhaar Lookup

This module shall allow the members to know the status of Aadhaar mapping in the Aadhaar Payment Bridge (APB) system and can be used for verification of a list of Aadhaar numbers through an upload process and response thereof. This would help the members to process Direct Benefits Transfer (DBT) transactions more efficiently and help reduce returns.

Sl#	Functional Requirements
FR01	Provision for seeding respective Aadhaar number of beneficiaries in the respective bank accounts.
FR02	Provision for uploading all the relevant details on the NPCI mapper by the member Banks at the end of day on daily basis.
FR03	Provision to make necessary arrangements to enable the bank staff as well as the customer to check the Aadhaar mapping status.
FR04	Shall have provision for the Government departments or the sponsor banks to check the seeding status of the Aadhaar number.
FR05	Shall have provision to use the lookup option to know the status in case of bulk and Aadhaar look up facility shall be availed from NPCI to ascertain mapping status of a batch of Aadhaar numbers.

Sl#	Functional Requirements
FR06	Provision of Verification of Aadhaar number and linking the same to the customer’s account in core banking system of the bank.
FR07	Shall have provision of verifying the account is eligible to receive the credits pertaining to the direct benefit transfers and if the account is not eligible to receive the DBT related credit then the seeding request shall be returned to the customer with appropriate reason.

5.8 Integration with Departmental Schemes

During the integration of Aadhaar Authentication framework with any departmental scheme, the SI shall conduct the following activities.

Sl#	Functional Requirements
FR01	Provision for discussion on integration process and modalities with the software implementation agency who will integrate in the application with Aadhaar Authentication Framework
FR02	Shall have provision to guide the process of authentication on different technical requirements
FR03	Shall provide functionalities of the pre-production AUA service URL and guide the process of implementation
FR04	Shall have provision to give guideline on understanding of authentication API
FR05	Shall have functionalities for AUA to provide the final production URL with Sub-AUA code for production access, after successfully tested into pre-production environment
FR06	Shall have functionalities of end to end integration support and give the solution if any error occurs during integration

5.9 Scheme on-boarding and authentication framework

Sl#	Functional Requirements
FR01	The system shall have provision for providing interface of the application of the various existing Departments of Government of Odisha and India to

Sl#	Functional Requirements
	UID-software system for identification verification and validation of the beneficiaries.
FR02	The Aadhaar enabled department Database shall be used for verification and validation of beneficiaries through CIDR database managed by UIDAI.
FR03	The Application shall implement solution for Aadhaar Authentication using Authentication API; existing User Departments may adopt Aadhaar Authentication into their applications with minimalistic configuration changes.
FR04	System shall have provision of repository of services may be used by the departments as a service to verify the document digitally for various Government schemes / services.

5.10 ASA Service Management

ASA is any entity that transmits authentication requests to the CIDR on behalf of one or more AUAs. They play the role of enabling intermediaries. They have an established secure connection with the CIDR and convey AUAs' authentication requests to the CIDR. ASAs receive CIDR's response and transmit the same back to the AUA. The SI should responsible for all API integrations of ASA as and when required. The SI also should have implement multiple ASAs in authentication ecosystem. Functional requirements for ASA service management are as follows.

Sl#	Functional Requirements
FR01	The SI shall comply with UIDAI and ASA guidelines for entire proposed solution as per the needs specified by UIDAI and ASAs.
FR02	In case one ASA is down, the system shall have the capabilities to reroute the request via other alternate ASAs. There must be provision for digitally signing the Auth XML requests on behalf of AUA. The Auth XML should append the AUA code along with the request. The Auth XML should be sent to ASA over the secured network. For the response that is received from ASA, should be forwarded to specific AUA from where the request originated.
FR03	Shall have the provision for management of ASA License keys.
FR04	Shall have the provision to provide required support to end customers for ASA services as per SLA.

Sl#	Functional Requirements
FR05	Shall have provision of log and maintain details of all authentication transactions.

5.11 Aadhaar Data Vault enhancements

Aadhaar Data Vault is a centralized storage for all the Aadhaar numbers collected by the AUAs/KUAs/Sub-AUAs/ or any other agency for specific purposes under Aadhaar Act and Regulations, 2016. It is a secure system inside the respective agency's infrastructure accessible only on need to know basis.

Sl#	Functional Requirements
FR01	Provision to have complete migration of Aadhaar Data Vault Solution.
FR02	Shall have provision in audit of the Aadhaar Authentication Framework as per UIDAI checklist once a year through any valid Cert-in empanelled vendor.
FR03	Shall have provision for Integration and implementation of Aadhaar Data Vault at all Sub-AUA applications.
FR04	Shall have provision of regular monitoring of database performance issues, errors, transaction analysis
FR05	Shall have Provision for optimization of database queries and procedures
FR06	Shall have provision for Support to Sub-AUAs in Integration of Encryption and Decryption service of Aadhaar Data Vault.
FR07	Shall have provision in handling of complete encrypted data at the time of Encryption Certificate Expiration
FR08	Provision for updation in Data Vault application workflow as per new requirements by UIDAI or system.
FR09	Shall have provision in execution of regular Security Audit of application by OSDC.

5.12 Enhancement of FIR Service as per UIDAI guidelines

a) FMR - The biometric data is of type "Fingerprint Minutiae Record". This data is in ISO minutiae format with no proprietary extensions allowed.

b) FIR - The biometric data is of type “Fingerprint Image Record”. The data is a fingerprint image packaged in ISO 19794-4 format, which could contain a lossy compressed image of type Jpeg2000.

Sl#	Functional Requirements
FR01	Shall have provision to ensure security of transactions during biometric authentication process from FMR only to FIR and FMR as per its circular dated 11.11.2021 and 03.02.2022.
FR02	AUA needs to do necessary changes in applications in consultation with corresponding device providers to enable transmission of FMR and FIR in the same authentication request in compliance to UIDAI guidelines.
FR03	Sub-AUA applications shall also be required to make same changes in their respective applications.

5.13 Supply of Hardware Security Modules (HSM)

Hardware Security Modules (HSM) & associated Software

a) Supply, install and maintain the Hardware Security Module (HSM) at the locations specified by OCAC
b) Store the private keys used for digital signing of Auth XML and Decryption of electronic “know your customers” (e-KYC) data received from UIDAI
c) Store document signer certificates for digital Invoice signing
d) Should maintain high availability within data centre
e) Supply updates and upgrades including new versions of all the software licenses supplied as part of this tender during the entire contract period
f) MAF (Manufacturer Authorization Form) with a provision of on-site support for 5 years
g) The **Technical Specification** of HSM is given below

Sl#	Description of Requirements	Compliance (Yes/ No)	Remarks
Functional Capabilities			
1.	Must support cryptographic offloading and acceleration		
2.	Should provide Authenticated multi-level access control (remote and local), Protection for configurability using secure devices such as USB		

Sl#	Description of Requirements	Compliance (Yes/ No)	Remarks
	token, Roles - Support for role based access control (minimum 2 roles)		
3.	Must have strong separation of administration and operator Roles		
4.	Capability to support client authentication using strong cryptographic technique and the secure channel should be terminated at the cryptographic processor and not to the HSM chassis.		
5.	Must have secure key wrapping, backup, replication and Recovery using a FIPS 140-2 compliant backup HSM		
6.	Must support protected key storage inside the FIPS 140-2 Level3 cryptography boundary throughout the key lifecycle		
7.	Must support clustering and load balancing without the need for any external load balancer		
8.	Should support Logical cryptographic separation of application keys		
9.	Must support —M of N multi-factor authentication via PED for enhanced security support		
10.	Supported Operating Systems - Windows, Linux, Solaris, AIX, HP-UX etc.		
11.	Support of Functionality Modules to run custom code within the secure boundary of the FIPS 140-2 Level 3 certified HSM.		
12.	Support of Functionality Modules to run custom code within the secure boundary of the FIPS 140-2 Level 3 certified HSM.		
13.	There should be no root or super-user access to HSM appliance possible in any way. No access to bash , ksh or any default terminal shells should be possible.		

Sl#	Description of Requirements	Compliance (Yes/ No)	Remarks
14.	The proposed HSM should ensure seamless migration of existing keys with upmost security without taking the keys out in plain format as well no separate downtime requirement.		
15.	The proposed HSM should also ensure that the existing application continue to work without any change in the code.		
16.	Support for migration of existing keys from current HSM through high availability or through G5 backup device .		
17.	Should Support remote administration for maintaining partitions and adding or removing partitions as business required without the need for accessing HSM physically in DC.		
Application Program Interfaces (APIs)			
18.	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, REST API, JCPROV for administration		
Host Connectivity			
19.	Dual Gigabit Ethernet ports (to service two network segments) with support for port bonding		
Cryptography			
20.	Asymmetric public key algorithms: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA		
21.	Symmetric algorithms: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST		
22.	Hash/message digest: SHA-1, SHA-2, SHA-3, SM2, SM3, SM4		
23.	Full Suite B implementation with fully licensed ECC including Brainpool and custom curves, supported out of the box without any additional license		

Sl#	Description of Requirements	Compliance (Yes/ No)	Remarks
Security compliance			
24.	FIPS 140-2 Level 3 with certification on manufacturer's name (Proposing third party FIPS 140-2 l3 certification will not be considered)		
25.	Common Criteria EAL4+ (AVA_VAN.5 and ALC_FLR.2) against the Protection Profile EN 419 221-5, with certification on manufacturer’s name (Proposing third party Common Criteria certification will not be considered)		
26.	Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS compliance		
Safety and environmental compliance			
27.	Compliance to UL, CE, FCC part 15 (for Commercial products), India BIS		
28.	Compliance to RoHS2, WEEE		
Management and monitoring			
29.	Support Remote Administration —including adding applications, updating firmware, and checking the status— from NoC		
30.	Syslog diagnostics support		
31.	Command line interface (CLI)/graphical user interface (GUI)		
32.	Support SNMP monitoring agent		
Physical characteristics			
33.	Standard 1U 19in. rack mount		
Performance			
34.	RSA 2048 bit signing performance 5,000/second and RSA 2048 key generation performance min 10 keys/second from a single box.		

Sl#	Description of Requirements	Compliance (Yes/ No)	Remarks
35.	ECC 256 bit prime curve signing performance 10000 /sec and ECC 256 bit key generation performance - 80/sec		
Custom Application			
36.	Should enable secure execution of custom security-critical application code within the tamper resistant hardware boundary		
Key Generation and Protection			
37.	Ability to generate RSA keys (2048 and 4096) on board on demand and shall be secured inside the high security module in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation from a single box.		
Key back up and restoration			
38.	The proposed solution must include the software/hardware to - securely store the keys at DC, at DR and at one remote location and restore them in accordance with FIPS 140-2 Level 3 without taking the keys in plain, in case of necessity		
Key Storage Area			
39.	The HSM must secure keys inside the HSMs FIPS 140-2 Level3 cryptography boundary throughout the key lifecycle		
Instant Key reflection			
40.	Multiple HSMs to be supportable for DR, key backup, key update, and key processes, load balancing and failover. Should support instant key reflection to all the HSMs in the System without the need for any external load balancer		
Logical partitions			

Sl#	Description of Requirements	Compliance (Yes/ No)	Remarks
41.	Number of Partitions Expandable up to 20 within HSM		
Warranty			
42.	OEM should have support centre in India & should have 25+ employees in its Payroll.		
43.	The OEM should have their own warehouse in India so that any Hardware support (RMA) can be provided easily & without any delay		
44.	OEM should be supplying in India for more than 10 years		

5.14 Supply and Installation of Database License and Support

a) Supply and Installation of ORACLE licenses in the ExaCC hardware available at Odisha State Data Center. All licenses shall be perpetual in nature.

b) Providing updates, patches and support for six (6) years from the date of delivery of license.

c) Hire the PaaS Services of ExaCC from ORACLE considering the above licenses for the specified period.

d) Configure the Database instance at ExaCC

e) Testing the environment

f) Migrate the Database from existing environment to ExaCC

5.14.1 OEM (Oracle) Technical Support for Database

Deployment of OEM technical resource (database administrator) onsite in OCAC officer for a period of 6 Months (3 Months Development and 3 Months post go-live) during all Government working hours.

The Onsite database Administrator shall be required to undertake the responsibilities of system administrator and troubleshooting of cloud based and on-premises infrastructure. The Database Administrator shall OEM certified and should be directly from M/s ORACLE India Private Limited (or Oracle India Consulting) .

5.14.1.1 Qualification

a) Any Graduate, Preferred B.E/ B.Tech/ MCA/ M.Tech

b) 8 Years of experience on ORACLE Database Administration

c) ORACLE Certification in Database Platform

d) Practical experience of latest version of Oracle RDBMS

5.14.1.2 Experience in following activities

a) Installing and upgrading the Oracle server and application tools (necessary update and patches)

b) Allocating system storage and planning future storage requirements for the database system

c) Creating primary database storage structures (table spaces) after application developers have designed an application

d) Creating primary objects (tables, views, indexes) once application developers have designed an application

e) Modifying the database structure, as necessary, from information given by application developers

f) Enrolling users and maintaining system security

g) Controlling and monitoring user access to the database

h) Monitoring and optimizing the performance of the database

i) Planning for backup and recovery of database information

j) Maintaining archived data on tape

k) Backing up and restoring the database

l) Contacting Oracle Corporation for technical support

m) Real Application Clusters, Configuration & Manage

Annexure-I

Compliance Checklist

Sl. No	Clause No	Details/Description
Aadhaar (Authentication) Regulations 2016		
1	5(2)	5. Information to the Aadhaar number holder.— (1) At the time of authentication or Offline Verification, a requesting entity or Offline Verification Seeking Entity (OVSE) respectively shall inform the Aadhaar number holder or in case of a child, inform the parent or guardian, of the following details:— the nature of information that will be shared by the Authority upon authentication with the requesting entity; the uses to which the information received during authentication or offline verification may be put; and alternate and viable means of submission of identification and that no service to the resident will be denied for refusing to, or being unable to, undergo authentication or offline verification. (2) A requesting entity shall ensure that the information referred to in sub-regulation (1) above is provided to the Aadhaar number holder in local language as well. (3) A requesting entity or OVSE shall ensure that the no service is denied to any resident for refusing to or being unable to undergo authentication or offline verification provided that the resident is able to identify himself through a viable alternative means as suggested by the requesting entity under sub-regulation (1) (c) above.
2	6	6. Consent of the Aadhaar number holder.— After communicating the information in accordance with Regulation 5, a requesting entity or Offline Verification Seeking Entity (OVSE) shall obtain the consent of the Aadhaar number holder

		or in case of a child, the consent of the parent or guardian of the child for the authentication or verification. A requesting entity or OVSE shall obtain the consent referred to in sub-regulation (1) above in physical or preferably in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.
3	7 (1), (2)	7. Capturing of biometric information by requesting entity— (1) A requesting entity shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by the Authority. (1a) All biometric devices used for authentication shall be Registered Devices as per the standards specified by the Authority from time to time. (1b) All the biometric devices shall be registered with the server of the requesting entity. (2) A requesting entity shall necessarily encrypt and secure the biometric data at the time of capture as per the specifications laid down by the Authority. (3) For optimum results in capturing of biometric information, a requesting entity shall adopt the processes as may be specified by the Authority from time to time for this purpose.
4	8 (1), (2)	8. Devices, client applications, etc. used in authentication.— All devices and equipment used for authentication shall be certified as required and as per the specifications issued, by the Authority from time to time for this purpose. The client applications i.e. software used by requesting entity for the purpose of authentication, shall conform to the standard APIs and specifications laid down by the Authority from time to time for this purpose.
5	9 (1), (5)	9. Process of sending authentication requests.—

		(1) After collecting the Aadhaar number or any other identifier provided by the requesting entity which is mapped to Aadhaar number and necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application shall immediately package and encrypt these input parameters into PID block before any transmission, as per the specifications laid down by the Authority, and shall send it to server of the requesting entity using secure protocols as may be laid down by the Authority for this purpose. (2) After validation, the server of a requesting entity shall pass the authentication request to the CIDR, through the server of the Authentication Service Agency as per the specifications laid down by the Authority. The authentication request shall be digitally signed by the requesting entity and/or by the Authentication Service Agency, as per the mutual agreement between them. (3) Based on the mode of authentication request, the CIDR shall validate the input parameters against the data stored therein and return a digitally signed Yes or No authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data, as the case may be, along with other technical details related to the authentication transaction. (4) In all modes of authentication, the Aadhaar number is mandatory and is submitted along with the input parameters specified in sub-regulation (1) above such that authentication is always reduced to a 1:1 match. (5) A requesting entity shall ensure that encryption of PID Block takes place at the time of capture on the

		authentication device as per the processes and specifications laid down by the Authority.
6	14 (1) (a), (c), (d), (e), (f), (g), (h), (i), (j), (k), (l), (m), (n)	14. Roles and responsibilities of requesting entities. — (1) A requesting entity shall have the following functions and obligations:— (a) establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication; (b) establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests; (c) ensure that the network connectivity between authentication devices and the CIDR, used for sending authentication requests is in compliance with the standards and specifications laid down by the Authority for this purpose; (ca) ensure that the Aadhaar number/Virtual ID/ANCS Token provided by the resident for authentication request shall not be retained by the device operator or within the device or at the AUA server(s); (cb) ensure that the provision of authentication using Virtual ID is provided; (d) employ only those devices, equipment, or software, which are duly registered with or approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose; (e) monitor the operations of its devices and equipment, on a periodic basis, for compliance with the terms and conditions, standards, directions, and specifications, issued and communicated by the Authority, in this regard, from time to time,

		(f) ensure that persons employed by it for performing authentication functions, and for maintaining necessary systems, infrastructure and processes, possess requisite qualifications for undertaking such works. (g) keep the Authority informed of the ASAs with whom it has entered into agreements; (ga) obtain approval from the Authority before appointing any third party entity as Sub-AUA/Sub-KUA. (h) ensure that its operations and systems are audited by information systems auditor certified by a recognised body on an annual basis to ensure compliance with the Authority’s standards and specifications and the audit report should be shared with the Authority upon request; (i) implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to the residents; (j) in case of any investigation involving authentication related fraud(s) or dispute(s), it shall extend full cooperation to the Authority, or any agency appointed or authorised by it or any other authorised investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resources or information as well to assist the Authority in disseminating information to the general public about any Aadhaar data related fraud to enable Aadhaar number holders to evaluate whether they were victims of the fraud and take remedial action; (k) in the event the requesting entity seeks to integrate its Aadhaar authentication system with its local authentication system, such integration shall be carried out in compliance with standards and specifications issued by the Authority from time to time;

		(l) shall inform the Authority of any misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within their network. If the requesting entity is a victim of fraud or identifies a fraud pattern through its fraud analytics system related to Aadhaar authentication, it shall share all necessary details of the fraud with the Authority as well as to affected Aadhaar number holders without undue delay; (m) shall be responsible for the authentication operations and results, even if it sub-contracts parts of its operations to third parties. The requesting entity is also responsible for ensuring that the authentication related operations of such third party entities comply with Authority standards and specifications and that they are regularly audited by approved independent audit agencies; (ma) may agree upon the authentication charges for providing authentication services to its customer, with such customer, and the Authority shall have no say in this respect, for the time being; however, the Authority's right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved; (mb) Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters shall be masked by the requesting entity by redacting the first 8 digits of the Aadhaar number before storing the physical copies. (n) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority, for the purposes of using the authentication facilities provided by the Authority. (o) shall take specific permission of the Authority and sign appropriate agreement with the Authority, if requiring storage of Aadhaar number for non-authentication purposes. Aadhaar number

		shall be stored in a secure manner as specified by the Authority from time to time (p) extend full co-operation to the Authority for any mass awareness programmes that the Authority may undertake to sensitize Aadhaar number holders about the nature of data being used in authentication, the scope of misuse as well as steps to protect against such misuse or fraud
7	15 (2), (3), (4)	15. Use of Yes/ No authentication facility.— (1) A requesting entity may use Yes/ No authentication facility provided by the Authority for verifying the identity of an Aadhaar number holder for its own use or on behalf of other agencies. (2) A requesting entity may permit any other agency or entity to perform Yes/ No authentication by generating and sharing a separate license key for every such entity through the portal or any other mechanism provided by the Authority to the said requesting entity. For the avoidance of doubt, it is clarified that such sharing of license key is only permissible for performing Yes/ No authentication, and is prohibited in case of e-KYC authentication. (3) Such agency or entity: a. shall not further share the license key with any other person or entity for any purpose; and b. shall comply with all obligations relating to personal information of the Aadhaar number holder, data security and other relevant responsibilities that are applicable to requesting entities. (3A) AUAs/KUAs/Sub-AUAs/Sub-KUAs shall use their client application for Aadhaar authentication which shall be digitally signed by the requesting entity. (4) It shall be the responsibility of the requesting entity to ensure that any entity or agency with which it has shared a license key, complies with the provisions of the Act, regulations, processes,

		standards, guidelines, specifications and protocols of the Authority that are applicable to the requesting entity. (5) The requesting entity shall be jointly and severally liable, along with the entity or agency with which it has shared a license key, for non-compliance with the regulations, processes, standards, guidelines and protocols of the Authority.
8	16 (2), (3), (4), (5), (8)	16. Use of e-KYC authentication facility.— (1) A KUA may use the e-KYC authentication facility provided by the Authority for obtaining the e-KYC data of the Aadhaar number holder for its own purposes. (2) A KUA shall obtain specific permission from the Authority by submitting an application for sharing of e-KYC data with Sub-KUA and such data may be shared in encrypted form as per the guidelines issued by the Authority from time to time, with specific consent of Aadhaar number holder. (3) The Sub-KUA with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall not share it further with any other entity or agency. (4) The Aadhaar number holder may, at any time, revoke consent given to a KUA/Sub-KUA for storing his e-KYC data, and upon such revocation, the KUA/Sub-KUA shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder. (5) In addition to the restriction on further sharing contained in sub-regulation (3), all other obligations relating to the personal information of the Aadhaar number holder, data security and other relevant responsibilities applicable to requesting entities, shall also apply to the Sub-KUA with whom e-KYC data has been shared in accordance with this regulation 16.

		(6) The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with Sub- KUAs, for a period specified by the Authority. 16A. Use of Offline Verification facility.— (1) An OVSE may use the Offline Verification facility provided by the Authority for obtaining the offline Aadhaar data of the Aadhaar number holder only for the purpose specified to the Aadhaar number holder at the time of verification. (2) No entity shall perform Offline Verification on behalf of another entity or person. (3) An OVSE may store, with consent of the Aadhaar number holder, offline Aadhaar data of the Aadhaar number holder, received upon Offline Verification, securely as per the guidelines issued by the Authority from time to time. (4) The Aadhaar number holder may, at any time, revoke consent given to an OVSE for storing his/her offline Aadhaar data, and upon such revocation, the OVSE shall delete the offline Aadhaar data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder. (5) The Authority in cases of default or breach or change in law or any other circumstance as may be deemed appropriate by it, may direct the OVSE to discontinue the use of Offline Verification services.
9	17 (1) (a), (b), (c), (d), (e), (f), (g)	17. Obligations relating to use of identity information by requesting entity.— (1) A requesting entity shall ensure that: (a) the core biometric information collected from the Aadhaar number holder is not stored, shared or published for any purpose whatsoever, and no copy of the core biometric information is retained with it; (b) the core biometric information collected is not transmitted over a network without creation of encrypted

		PID block which can then be transmitted in accordance with specifications and processes laid down by the Authority. (c) the encrypted PID block is not stored, unless it is for buffered authentication where it may be held temporarily on the authentication device for a short period of time, and that the same is deleted after transmission; (d) identity information received during authentication is only used for the purpose specified to the Aadhaar number holder at the time of authentication, and shall not be disclosed further, except with the prior consent of the Aadhaar number holder to whom such information relates. (e) the identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected against access, use and disclosure not permitted under the Act and its regulations; (f) the private key used for digitally signing the authentication request and the license keys are kept secure and access controlled; and (g) all relevant laws and regulations in relation to data storage and data protection relating to the Aadhaar- based identity information in their systems, that of their agents (if applicable) and with authentication devices, are complied with.
10	18 (1), (2), (3), (4), (5), (6)	18. Maintenance of logs by requesting entity. — (1) A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:— (a) specified parameters of authentication request submitted excluding Aadhaar number, Virtual ID, ANCS Token or UID token; (b) specified parameters received as authentication response including full Aadhaar number or masked

		Aadhaar, as the case may be; (c) the record of disclosure of purpose for which the authentication was performed, to the Aadhaar number holder or parent or guardian, in case of a child, at the time of authentication; and (d) record of consent of the Aadhaar number holder, or parent or guardian, in case of a child, for authentication, but shall not, in any event, retain the PID information. (2) The logs of authentication transactions shall be maintained by the requesting entity for a period of 2 (two) years, during which period an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified. (3) Upon expiry of the period specified in sub-regulation (2), the logs shall be archived for a period of five years or the number of years as required by the laws or regulations governing the entity, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained upon the order of a court not inferior to that of a Judge of a High Court or required to be retained for any pending disputes. (4) The requesting entity shall not share the authentication logs with any person other than the concerned Aadhaar number holder upon his/her request or for grievance redressal and resolution of disputes or upon the order of a court not inferior to that of a Judge of a High Court. The authentication logs shall not be used for any purpose other than those stated in this sub-regulation. (5) The requesting entity shall comply with all relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.

		(6) The obligations relating to authentication logs as specified in these regulations shall continue to remain in force despite termination of appointment in accordance with these regulations.
11	21 (3)	21. Audit of requesting entities, Authentication Service Agencies and Offline Verification Seeking Entities.— (1) The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including their Sub-AUAs and Sub-KUAs, Authentication Service Agencies and Offline Verification Seeking Entities, either by itself or through audit agencies appointed by it, to ensure that such entities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued by the Authority. (2) The Authority may conduct audits of the operations and systems of the entities referred to in sub-regulation (1), either by itself or through an auditor appointed by the Authority. The frequency, time and manner of such audits shall be as may be notified by the Authority from time to time. (3) An entity subject to audit shall provide full co-operation to the Authority or any agency approved and/or appointed by the Authority in the audit process, and provide to the Authority or any agency approved and/or appointed by the Authority, complete access to its procedures, records and information pertaining to services availed from the Authority. The cost of audits shall be borne by the concerned entity. (4) On identification of any deficiency by the Authority, the Authority may require the concerned entity to

		furnish necessary clarifications and/or information as to its activities and may also require such entity either to rectify the deficiencies or take action as specified in these regulations. (5) Notwithstanding anything contained in clause (4), and without prejudice to any action which may be taken under the Act, the Authority may initiate action under Regulation 25(1A) on identification of any deficiency pursuant to the audit conducted.
12	22 (4)	22. Data Security.— (1) Requesting entities and Authentication Service Agencies/OVSEs shall have their servers used for Aadhaar authentication request formation and routing to CIDR/Offline Verification respectively, to be located within data centres or cloud storage centres located in India. (1A) Authentication requests shall not be accepted from entities located outside the territorial borders of India. For allowing authentication requests from outside India, the requesting entity shall take specific permission from the Authority. (2) Authentication Service Agency shall establish dual redundant, secured leased lines or MPLS connectivity with the data centres of the Authority, in accordance with the procedure and security processes as may be specified by the Authority for this purpose. (3) Requesting entities shall use appropriate license keys to access the authentication facility provided by the Authority only through an ASA over secure network, as may be specified by the Authority for this purpose. (4) Requesting Entities, Authentication Service Agencies and Offline Verification Seeking Entities shall adhere to all regulations, information security policies, processes, standards, specifications and guidelines issued by the Authority from time to time.
Agreement Terms and Conditions made between OCAC and UIDAI		

13	Terms and conditions of Appointment of Authentication User Agency (AUA)	4.1 UIDAI hereby grants the Authentication User Agency a non-exclusive and revocable right to use Aadhaar Authentication Services, for providing Aadhaar Enabled Services to Aadhaar Holder(s), in the manner set out in this Agreement. The Authentication User Agency understands and agrees that it shall be responsible to UIDAI for all its Aadhaar authenticationrelated aspects, covered by this Agreement, and in the event, the Authentication User Agency outsources part(s) of its operations to other entities, the ultimate responsibility for the results of Aadhaar authentication-related operations lies with the Authentication User Agency, and the Authentication User Agency shall ensure that the entity to which it has outsourced its operations is audited annually by an information systems auditor certified by a UIDAI recognized body. The Authentication User Agency also understands and agrees that it shall be responsible to UIDAI for all the Aadhaar authentication-related aspects for all authentication requests which it transmits to the CIDR on behalf of Sub AUAs appointed by it. For the avoidance of doubt, it is hereby expressly clarified that only entities contracted with UIDAI as an Authentication User Agency and their Sub AUAs shall be authorized to send a request for authentication of PIDs of the Aadhaar holders. All the obligations of the Authentication User Agency under this Agreement shall be equally applicable to the Sub AUAs. The Authentication User Agency understands that the Aadhaar Authentication Service shall be provided at the sole discretion of UIDAI, which reserves the right to add, revise, suspend in whole, or in part any of the Aadhaar Authentication Service, at any time with prior notice, in its sole discretion, for any reason whatsoever. 4.2 In case of an Authentication User Agency outsources or sub-contracts any part of its operations to another agency, it shall sign a sub-contracting undertaking with that Agency. This

		undertaking shall include all respective obligations (including security of Aadhaar numbers and other identifying information as applicable) under this agreement, the Act and Regulations. UIDAI may define a standard sub-contracting undertaking template from time to time and the Authentication User Agency shall be obligated to comply with the terms of the undertaking. 4.3 It is hereby mutually agreed between the Parties that the rights and obligations of the Authentication User Agency, under this Agreement, are non-transferable and non-assignable whether by sale, merger, or by operation of law, except with the express written consent of UIDAI. 4.4 The Authentication User Agency hereby unequivocally agrees that it shall use the Aadhaar Authentication Services, for providing Aadhaar Enabled Services to Aadhaar Holder(s), solely in terms of this Agreement. 4.5 The Authentication User Agency shall ensure that the client application to be used by Sub AUA for Aadhaar authentication is developed and digitally signed by Authentication User Agency or else Authentication User Agency shall give its digitally signed SDK (Software Development Kit) to Sub AUA for the purposes of capturing Aadhaar number and other authentication details such as demographics, OTP or biometrics. Under no circumstances, Sub AUA shall capture Aadhaar number and other authentication data for the purposes of Aadhaar Authentication by any means other than these two means described above. In addition, under no circumstances, Authentication User Agency shall expose the Aadhaar Authentication API directly to any other agency or application and only Authentication User Agency provided client application or SDK must access these APIs in a secure fashion. The Authentication User Agency

		shall also ensure that the Sub AUA client application or SDK, as the case may be, used for Aadhaar Authentication, is audited at the time of the creation of the application/SDK and also for every major release of the application/SDK or every year thereafter whichever comes first, by information systems auditor(s) certified by STQC / CERT-IN and the compliance audit report is submitted to UIDAI.
14	5. Obligations of the authentication user agency (AUA)	5.1 The Authentication User Agency hereby unequivocally agrees that it shall, forthwith, upon appointment as an Authentication User Agency, shall establish network connectivity, through an Authentication Service Agency, duly approved by UIDAI and employ only those devices, equipment or software, which are duly registered or certified by the Authority, monitoring their operations on a periodic basis. The AUA shall establish and maintain necessary authenticationrelated operations, including their own systems, processes, infrastructure, technology, security, etc., which is necessary for providing Aadhaar Enabled Services. The Authentication User Agency hereby expressly agrees to comply with all the Roles and Responsibilities under Regulation 14 of the Aadhaar (Authentication) Regulations, 2016. 5.2 The Authentication User Agency shall ensure that its operations and systems in terms of this Agreement are audited by information systems auditor certified by a UIDAI recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the audit report should be shared with UIDAI annually In addition to the above, UIDAI may choose to, in its sole discretion, to audit the AUA's operations and systems in terms of this Agreement by itself or through a certified auditor appointed by UIDAI, and the continuation of operations as the Authentication User Agency shall, at all times, be dependent upon the said audit confirming the compliance by the Authentication User Agency of

		the terms and conditions contained in this Agreement, and any failure in compliance of the same, if confirmed in the audit, may entail fine and/or penalties and termination of access to Aadhaar Authentication Services. 5.3 UIDAI from time to time may come up with different standards and certification schemes for AUAs, authentication / eKYC applications being used by AUAs, individual auditors responsible for audits, and the business correspondents / operators used by AUAs. The AUA shall ensure compliance to these standards and certification schemes as notified by UIDAI from time to time. 5.4. The Authentication User Agency unequivocally agrees to provide full cooperation to UIDAI or any agency approved and/or appointed by UIDAI in the audit process, and to provide to UIDAI or any agency approved and/or appointed by UIDAI, complete access to its procedures, records and information pertaining to services availed for UIDAI.
15	7. Confidentiality, data protection, security and use of information	7.1 The Authentication User Agency, all it’s Sub AUAs and all its Sub-contractors shall treat all information, which is disclosed to it as a result of the operation of this Agreement, as Confidential Information, and shall keep the same confidential, maintain the secrecy of all such information of confidential nature and shall not, at any time, divulge such or any part thereof to any third party except as may be compelled by any court or agency of competent jurisdiction, or as otherwise required by law, and shall also ensure that same is not disclosed to any person voluntarily, accidentally or by mistake. 7.2 The Authentication User Agency hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the Authentication User Agency, as a result of the

		operation of this Agreement, is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof, including all obligations relating to the protection of information under the Act. 7.3 It is hereby mutually agreed between the parties that UIDAI assumes no responsibility or liability for any action or omission, use or misuse, etc. of the Confidential Information and other data in the control and/or possession of the Authentication User Agency or its sub-AUAs or sub-contractors. 7.4 It is hereby mutually agreed that this Clause shall survive the expiry or termination of this Agreement. 7.5 The Authentication User Agency shall maintain the highest level of secrecy, confidentiality, and privacy with regard thereto. 7.6 Additionally, Authentication User Agency shall keep confidential all the details and information with regard to Aadhaar Authentication Services, including systems, facilities, operations, management and maintenance of the systems/facilities. 7.7 UIDAI shall retain all rights to prevent, stop and if required take the necessary punitive action against the Authentication User Agency regarding any forbidden disclosure. 7.8 For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information: information already available in the public domain; information which has been developed independently by the Authentication User Agency; information which has been received from a third party who had the right to disclose the aforesaid information; and

		Information which has been disclosed to the public pursuant to a court order. 7.9Any handover of the confidential information needs to be maintained in a list, both by UIDAI and Authentication User Agency, containing at the very minimum, the name of provider, recipient, date of generation of the data, date of handing over of data, mode of information, purpose and signatures of both parties.