RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

LIMITED TENDER DOCUMENT

FOR

Selection of Managed Service Partner (MSP) for Design, Supply, Installation, Configuration, Customization, Operations & Maintenance of Aadhaar Authentication Software Platform for ASA/AUA/KSA/KUA Services

Tender No. RailTel/Tender/LT/CO/DNM/2016-17/ASA-KSA/350 dated: 30.08.16

Tender Copy No._____

Sold to_____

Bid Data Sheet

SHORT TERM LIMITED TENDER NOTICE

Short Term Limited Tender Notice No. RailTel/Tender/LT/CO/DNM/2016-17/ASA-KSA/350 Dated 30.08.2016

RailTel Corporation of India Limited, Gurgaon, invites bids in sealed covers from reputed firms for **"Selection of Managed Service Partner for Design, Supply, Installation, Configuration, Customization, and Operations & Maintenance of Aadhaar Authentication Software Platform for ASA/AUA/KSA/KUA Services".**

" The details are as under: -

a)	**Last Date and Time of Submission of offer**	**Up to 15:00 hrs of 13.09.2016**
b)	**Time of opening of Limited Tender**	**15:30 hrs of 13.09.2016**
c)	**Validity of offer**	**60 days**
d)	**Delivery period**	**30 days**
e)	**Approximate value of the work**	**Rs. 1,20,000 /- (aprox.)**
f)	**Earnest Money (EMD):** **(To be deposited in the form of Bank Draft in favour of RailTel Corporation of India Limited, Gurgaon)**	**Rs. 2,400-** **(Two Thousand Four Hundred only).**
g)	Copy of Tender Document is enclosed herewith & also sent through email. All pages of original tender document duly signed by the tenderer along with the offer is to be submitted to this office at RailTel Corporation of India Ltd., Plot No. 143, Institutional Area, Opposite-Gold Souk, Sector-44, Gurgaon-122003.	
h)	For small scale units registered with NSIC under single point registration Scheme and participating in this tender enquiry, following exemptions are available:- They are exempted from depositing Earnest money These exemptions are applicable provided units are registered with NSIC for tendered item and registration is current and valid. Firms claiming these exemptions are required to submit along with their offer, copy of their current and valid NSIC registration certificate for the tendered item, otherwise their offer would not be considered.	

Pawan Kumar Sharma
Joint General Manager/DNM
For & on behalf of
RailTel Corporation of India Ltd.

INDEX

CHAPTER-1

Offer Letter

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

I/We _____ have read the various conditions detailed in tender document attached here to and hereby agree to ABIDE BY THE SAID CONDITIONS. I/We also agree to keep this tender open for acceptance for a period of 60 days from the date fixed for opening the same and in default thereof, I/We will be liable for forfeiture of my/our Earnest Money. I/We offer to do the **"Selection of Managed Service Partner (MSP) for Design, Supply, Installation, Configuration, Customization, Operations & Maintenance of Aadhaar Authentication Software Platform for ASA/AUA/KSA/KUA Services"** as per Schedule of Requirement for Limited tender No. **RailTel/Tender/LT/CO/DNM/2016-17/ASA-KSA/350 dated: 30.08.16** for RailTel Corporation of India Limited at the rates quoted in the attached schedules and hereby bind myself/ourselves to supply the Equipment within 60 days from the date of issue of Purchase Order. I/We also hereby agree to abide by the Various Conditions of PO and to carry out the supply according to the Specifications for materials laid down by the Railtel for the present order.

I agree for payment of Security Deposit or Performance Bank Guarantee as per terms & conditions of tender within 15 days after receipt of LOA to that effect.

SIGNATURE OF VENDOR (S)

Date

SIGNATURE OF WITNESS VENDOR (S) ADDRESS

1.
2.

CHAPTER 2

Eligibility criteria, Evaluation method and Schedule of Requirement

1.0 Objective of Work

RailTel through this tender will select Managed Service Partner for Design, Supply, Installation, Configuration, Customization, and Operations & Maintenance of Aadhaar Authentication Software Platform for ASA/AUA/KSA/KUA Services.

The intent of the tender is to invite eligible firms (who meet the qualification criteria as defined in Para 2.0 below) for selection of Managed Service Partner for Design, Supply, Installation, Configuration, Customization, Operations & Maintenance of Aadhaar Authentication Software Platform for ASA/AUA/KSA/KUA Services.

1.1 Introduction of Project

RailTel has become Authentication Service Agency (ASA), Authentication User Agency (AUA), KYC Service Agency (KSA) and KYC User Agency (KUA) of UIDAI to render Aadhaar based Authentication and e-KYC services to various customers, partners and stakeholders.

ASAs are entities that have established secure leased line connectivity with the CIDR (Aadhaar Database) compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies and transmit AUAs' authentication requests to CIDR. Only entities contracted with UIDAI as ASAs shall send authentication requests to the CIDR; no other entity can directly communicate with CIDR. An ASA could serve several AUAs; and may also offer value added services such as multi-party authentication, authorization and MIS d to AUAs. Once the Aadhaar ASA authentication application stack has been established, it can be used for serving multiple AUAs in future thereby expanding business with one-time setup.

AUA is any government / public / private legal agency registered in India that seeks to use Aadhaar authentication for its services. An AUA is the principal agency that sends authentication requests to enable its services / business functions. An AUA connects to the CIDR through an ASA (either by becoming ASA on its own or contracting services of an existing ASA).

The Aadhaar e-KYC API can be used (only with the explicit authorization of the resident through biometric/OTP authentication) by an agency to obtain latest resident demographic data and photo data from UIDAI. The resident servicing agency is called the KYC User Agency (KUA). The KUA accesses the e-KYC service through a KYC Service Agency (KSA). The KSA provides connectivity to the UIDAI's Central ID Repository (CIDR).

2. Eligibility Criteria for Bidder

2.1 The Bidder Company should be an Indian registered company or a subsidiary of a Global company, incorporated under the Indian Companies Act 1956.
Valid documentary proof of:

- Certificate of incorporation

- Certificate of Commencement
- Certificate consequent to change of name, if applicable
- Copy of Memorandum of Association
- Income Tax registration/PAN number

.

2.2 The Bidder should have developed and implemented ASA/KSA as well as AUA/KUA software/services for at least one organization in India (Central Government/State Government/PSU/Private Sector Company) and the implemented ASA / KSA software / service should be in production a period of atleast 12 months.

2.3 Bidder Company should be working for minimum one year at the time of submitting proposal in any of following related business domain:-

- Managing any Aadhaar Enabled Software Platform for Authentication and e-KYC Services such as Aadhaar Enabled Attendance Management System, Aadhaar Enabled Public Distribution System, Aadhaar Enabled Payment System, Aadhaar Enabled e-KYC System, etc.

2.4 Bidder should submit an undertaking that the bidder is not black listed by Central Government / State Government/ PSU in India.

The Bidders shall submit necessary documentary proof showing that they meet the eligibility criteria along with their bid. All documents submitted shall also be self-attested by the Bidder.

3.0 Evaluation Method

The evaluation will be done broadly in 10 parameters (9 Technical Criteria & 1 Commercial Criteria in the ratio 7:3) with weightage as defined below:-

A. Cumulative Turnover of last three financial years

SN	Cumulative turn over in last 3 years in Lakh (Rs.)	Marks
1	Less than 20	5
2	20-30	6
3	31-40	7
4	41-50	9
5	Above 50	10

B. Experience with Telecom Service Provider/Central Government/State Government/PSU (ASA/KSA/AUA/KUA)

SN	No. of TSP/Government/PSU Serving through Contracts/Agreements with Live ASA/KSA	Marks
1	1	5
2	2	6
3	3	7
4	4	9
5	More than 4	10

Bidder must provide the documentary proof/Copy of Agreements.

C. Experience in Implementation of UIDAI Application Platform for Aadhaar Enabled Services

SN	Years of Experience in Aadhaar Platform	Marks
1	Less than 0.5	5
2	0.5	6
3	1	7
4	2	9
5	3 or More than 3	10

D. Additional Experience with a number of potential customers (Live ASA/KSA) through agreements

SN	No. of Contracts/Agreements with Live ASA/KSA	Marks
1	1	5
2	2	6
3	3	7
4	4	9
5	More than 4	10

Bidder must provide the documentary proof/Copy of Agreements.

E. Experience in implementing Aadhaar API Specifications (Authentication Version 1.6, BFD Version 1.6, e-KYC Version 1.6, OTP Version 1.6, Mobile Update Version 1.0) with Live ASA/KSA

SN	No. of Aadhaar APIs Implemented with Live AUA/KUA	Marks
1	1	5
2	2	6
3	3	7
4	4	9
5	5	10

F. Additional Experience with a number of potential customers (Live AUA/KUA) through ASA/KSA agreements

SN	No. of AUA/KUA Serving through Contracts/Agreements with Live ASA/KSA	Marks
1	1	5
2	2	6
3	3	7
4	4	9
5	More than 4	10

Bidder must provide the documentary proof/Copy of Agreements.

G. Volume of Transactions carried out in Aadhaar Platform :-

SN	Volume of Transactions	Marks
1	Less than 10 Lakh	5
2	10-20 Lakh	6
3	20-30 Lech	7
4	30-40 Lakh	9
5	More than 40 Lakh	10

H. Profile of Leaders (Member of Board of Directors/Partner/CEO/Upper Management):-

SN	Total Years of Experience of All Directors	Marks
1	Less than 10	5
2	10-20	6
3	21-30	7
4	31-40	9
5	More than 40	10

I. Technical Team Size working on UIDAI Application Platform:-

SN	Team Size (No. of Employees)	Marks
1	Less than 3	5

2	4-5	6
3	6-8	7
4	9-10	9
5	More than 10	10

J. Schedule of Requirement (Commercial Criteria)

SN	Particulars of Service	MSP Quote in Percentage	Marks
1	Fixed Revenue Share per Aadhaar Transaction (Authentication, e-KYC, etc)		12%-10%=5 Marks 9%-10%=6 Marks 7%-8%=7 Marks 5%-6%=9 Marks 1%-4%=10 Marks
2	Tax		Statutory

Note:

1. Railtel shall negotiate the rates for every requirement in order to submit a competitive proposal to its prospective customers.
2. Revenue share percentage shall not exceed beyond 12%.
3. The revenue share will be included of all the taxes. No other payment will made above that.

The bidders must produce documentary evidence for above all evaluation criterion. Merit list will be prepared based on the marks obtained on evaluation criteria mentioned above and highest scorer bidder will be selected as Managed Service Partner (MSP) for Implementation of Aadhaar Authentication Software Platform for ASA/AUA/KSA/KUA Services.

CHAPTER 3

Introduction and Scope of work

1.0 Brief of RailTel

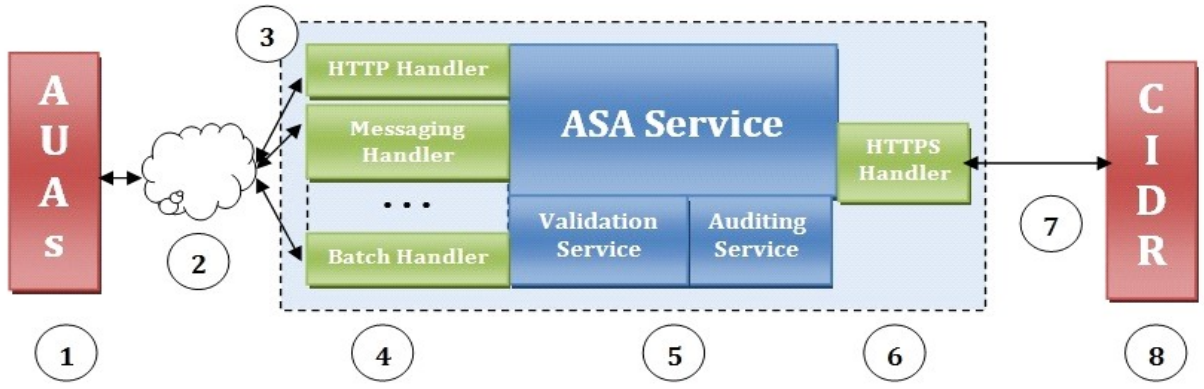
RailTel Corporation of India Limited, a Public Sector Undertaking under the Ministry of Railways, Govt. of India, and is a national telecom service provider having NLD, ISP and IP1licenses and have built nation-wide optical fiber network. RailTel's objective is to create a nation-wide broadband telecom and multimedia network.

RailTel Corporation of India Limited (RailTel) an ISO-9001:2000 organization is a Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to significantly contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

2.0 Brief about ASA/KSA

ASAs can offer AUAs multiple protocols and options for connecting their solution to Aadhaar system and in addition provide reporting and other value added services. If ASA is a telecom provider, then a full connectivity solution could be provided to an AUA for end to end Aadhaar authentication.

At a basic level, ASA service is- that of forwarding API calls from AUAs to CIDR through a secure connection. ASA server should be built like a middleware or enterprise service bus that allows secure incoming connections from AUAs to be verified, audited, and then invoking API URLs exposed by Aadhaar servers through HTTPS and then sending the response back to AUAs. A complete ASA server could be thought of as a middleware (or Enterprise Service Bus – ESB) providing multiple protocol support, multiple data format support, with built-in format translation and other capabilities such as auditing and reporting.



If ASAs wishes to offer multiple choices in terms of how AUAs actually communicate with ASA server, it is suggested that, a well-designed layer handling various protocols be built.

- A pluggable set of protocol handlers could provide standard protocols such as HTTPS, JMS, etc. to be used for incoming communication from AUA servers.

- In most cases, AUAs form the final API input XML and digitally sign them before sending it to ASA so that ASA server can forward that request to Aadhaar servers.
- In some cases, where ASA is a domain aggregator and offering value added services such as input XML creation, digital signature etc. to AUAs, a choice of data formats (XML, binary formats such as ISO-8583 in the case of financial transactions, JSON, csv, etc.) also could be offered to AUAs using a format translation scheme.
- In the above scenario, ASA is expected to digitally sign the API input XML on behalf of AUAs.

Once the data is received in the ASA server, servers needs to do the following:

- Validate the input data to ensure compliance to Aadhaar data definitions as well as to eliminate issues such as SQL-injection etc.
- Once it is validated, it needs to be formatted to an XML format complying with Aadhaar API specifications.
- After the API input XML is formed, it needs to be forwarded using HTTPS to Aadhaar servers hosted in CIDR (Central Identities Repository) as per API specification (see point below).
- Once response is received from Aadhaar servers, transaction needs to be audited into an audit database.
- Then the response XML needs to be formatted back to AUA specific format and sent back to AUA using an appropriate protocol adapter.

Protocol for communication between ASA server and Aadhaar servers at CIDR is always HTTPS.

- All Aadhaar APIs are exposed as a service over HTTPS.
- Data format for all Aadhaar APIs is XML.
- In most cases, ASAs need to simply forward the digitally signed API input XML to Aadhaar servers through HTTPS.

CIDR represents one or many UIDAI data centers where Authentication and related online services are made available.

- Aadhaar authentication related services are available in active-active mode (meaning request can be routed to any data center) across both data centers.
- UIDAI services are load balanced and routed internally without the knowledge of ASA to ensure maximum service availability.

2.1 Brief about AUA/KUA

AUA Technology Infrastructure

Similar to any other technology project, for implementation of Aadhaar authentication an AUA would need to set up the IT infrastructure. The following section lists the indicative resources (hardware, software, and manpower) required for building applications for processing Aadhaar authentication.

AUA Authentication Devices

- Authentication devices are expected to be used for a variety of purposes and would need to be specific to every AUA's requirements.

- Authentication request (Biometric/ Demographic/ OTP) could be initiated from any kind of device capable of creating authentication packet as per UIDAI's authentication APIs.
- For biometric authentication, sensor and extractor combination certified by STQC should be used in the devices.
- UIDAI specifications include sensor & image extractor requirements and device suitability to general Indian operating conditions. The specifications and the certification procedure may be accessed from STQC's website through this link – UIDAI Authentication Device Specifications.
- Besides the sensor-extractor specifications provided by UIDAI, AUAs may specify additional requirements such as multi language support, voice support, form factor etc. Various device vendors are expected to incorporate the certified sensor-extractors in device models / form factors based on AUA's needs. AUAs are expected to select form factor based on requirements such as
    - Service delivery and deployment needs i.e. level of Mobility is required etc.
    - Network availability in locations where devices are deployed, AUAs may also consider opting for solutions such as dual SIM, external antennas etc.
    - Suitability to specific environmental conditions such as, hot/cold desert, high humidity areas etc.

AUA Server Application Architecture

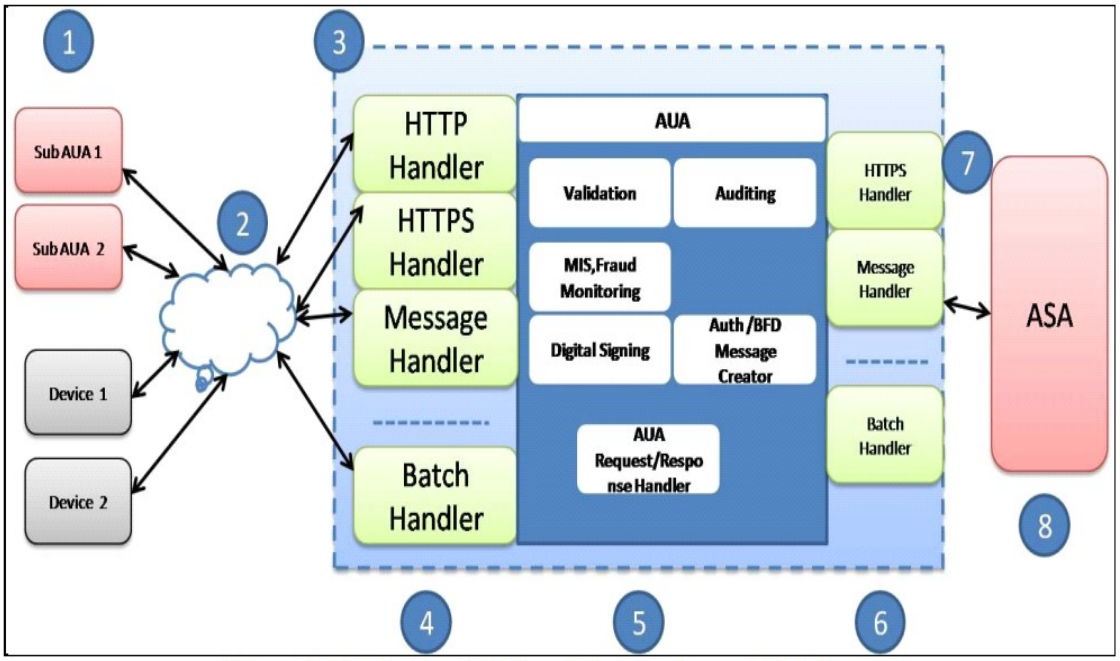


Figure 5: Illustrative High Level Architecture of AUA Server

At a high level the flow of API request and response is as follows (point number below corresponds to number within the circle above):

1. Multiple devices or Sub AUAs should be supported.
2. Connectivity between Sub AUAs and devices

3. Network connectivity from devices to AUA server (Internet, GPRS, Broadband etc) in a reliable, secure fashion.
4. Communication protocol can be the choice of AUA and Sub-AUA. Indicative options are mentioned in the diagram above (Figure 1).
5. To make communication more secure VPN option could also be used.(suggested option in case of a Sub AUA)
6. AUA server (depicted in the light blue box with dotted line border)
7. This should be built to support a "horizontally" scalable deployment on one or multiple servers, so that as the transaction volume increase, additional servers can be added to handle the load.
8. A generic AUA server should provide multiple protocol support as shown in the diagram above (providing AUAs a choice of protocols).

Components 4, 5, and 6 are parts of AUA server and are described below:

AUA Applications

AUA applications can use Biometric (Finger Print), Demographic and OTP (One Time PIN) based authentication in its business application. As shown in the architecture section above for all type of applications, solution should be modular and configurable. Module/Component based solution will help in making application loosely coupled and hence provide a lot of flexibility in maintenance and upgrades. It is recommended that business application is not tightly coupled with Authentication application. In all scenarios authentication will only form a part of the total solution, so authentication functionality should be ideally developed as a standalone service that could be consumed as and when required during the service delivery process.

For biometric authentication an AUA is required to build the following applications on the authentication devices:

- Best Finger Detection Application
- Finger Print Authentication application
- IRIS Authentication Application
- OTP

Implementation of the AUA Authentication Framework

1. Creation of a Web service with 5 web methods for each type of authentication, and is deployed on the server.

2. The Web service shall have the required web methods for calling the authentication event of the UID client sample application (as given by UIDAI). The web method shall take input parameters based on the type of authentication and shall also have a return variable which will denote success and failure (as per the return value from the authentication event).

3. The user applications which are willing to use authentication services need to call the corresponding web method of the web service and fetch the return variable for success and failure.

The Authentication and e-KYC Modules would work as a routing agent which shall check the validity of each authentication / e-KYC request and route the requests through the Aadhaar ecosystem to Central

Identities Data Repository (CIDR) through ASA/KSA. The response received from UIDAI shall be forwarded to respective clients acting as a Sub-AUA/KUA.

3.0 Scope of work

3.1 Application Software Requirements

Sl. No.	*Business / Functional Requirements*	*Mandatory / Desirable*
Generic Requirements		
1.	Upon successful service delivery by the Authentication/e-KYC module, the system should allow processing and forwarding of authentication requests in the format accepted by UIDAI (presently XML) between AUA application & CIDR and vice versa within reasonable round trip time mandated by UIDAI.	Mandatory
2.	Application developed should support for secure/encrypted communication between ASA/AUA and CIDR as per UIDAI standards.	Mandatory
3.	The authentication application platform must be forward compatible with any service and security standards proposed by UIDAI.	Mandatory
4.	The system should be in compliance with UIDAI specifications and standards published from time to time.	Mandatory
5.	All requests and responses should be logged. The logs shall capture details of authentication transaction but not corresponding Personal Identity Information (PID).	Mandatory
6.	The system should maintain a log and report for all transactions for audit purpose. Reporting of this module shall be integrated with the Dashboard Module.	Mandatory
7.	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/sub AUA from where the request originated.	Mandatory
8.	The Aadhaar authentication should carry out the following Aadhaar Biometric Authentication: • The system should route all biometric authentication requests from registered departmental applications (AUAs or Sub-AUAs) to CIDR and back; • The system should implement Authentication API • The system should authenticate residents fingerprint and iris	Mandatory
9.	The Aadhaar authentication should carry out the following Aadhaar OTP Authentication:	Mandatory

	The system should route all OTP authentication requests from registered departmental applications (Sub-AUAs) to CIDR and back. The system should implement OTP Authentication API. The system should authenticate residents with registered mobile numbers.	
10.	The system should handle Authentication API errors correctly.	Mandatory
11.	The solution should have interface to search and filter the data of the Report.	Mandatory
12.	The authentication module should support in establishing SSL connection between the communication systems.	Mandatory
13.	The Solution should provide for future scalability of the whole system without major architectural changes.	Mandatory
14.	Should support Web Interface.	Mandatory
15.	The solution should be highly scalable and capable of delivering high performance as & when transaction volumes / users increases without compromising on the response time.	Mandatory
16.	The application software platform for Aadhaar based Authentication and e-KYC services should be compatible with all the standard operating systems such as Windows, Linux, UNIX, etc. Major Software for ASA/KSA and AUA/KUA along with any auxiliary components such as Web Server, Application Server, Gateway Server, Load Balancer, etc must also be compatible / smoothly work with Windows, Linux, UNIX, etc.	Mandatory
17.	The solution shall run on native browser with additional plug-ins that should be freely downloadable and should support at the minimum IE, Firefox Mozilla Google Chrome etc.	Mandatory
18.	User Interface should require only standards compliant browsers with standard support for JavaScript and HTML.	Mandatory
19.	Should not require opening of any special protocols for connecting the user client to the web/ application server. All communication should be on secured HTTPS.	Mandatory
20.	The solution shall be supported on client with mobile based platform.	Mandatory
21.	The Application Platform must be compatible / interoperable with HSM Devices such as Thales, Safenet, etc and integration between HSM API and ASA/AUA/KSA/KUA application must be carried out free of cost.	Mandatory
22.	It should be possible to integrate/call/plug-in the ASA/AUA/KSA/KUA application as a module with other web-based/g-based applications.	Mandatory
23.	The web based application should comply with Guidelines for Indian Government Websites (GIGW), W3C and WCAG 2.0 Level A.	Mandatory
24.	The Railtel will be the owner of the source code of the complete developed platform.	Mandatory

25.	Bidder solution should provide Web based API for performing Authentication and eKYC and the hosted API page should have support majority of the STQC Certified Fingerprint and Iris biometric devices and should have already implemented the solution integrated with STQC certified biometric devices of atleast 3 different companies. The client side API should be available for Java, .NET and PHP Platform	Mandatory
26.	Bidder solution should have capability to sign / encrypt/ decrypt the Aadhaar xml's using Hardware Security Module of OEMs like Thales, Safenet, etc, USB Token and File based certificates.	Mandatory
27.	Bidder should have experience in interfacing with ASA Platform providers for Payment Systems, Data Repository, e-Governance Schemes, etc.	Mandatory
28.	Bidder solution should have the following API Specifications implemented and should be in use in a production environment at existing customer locations: a) AADHAAR AUTHENTICATION API SPECIFICATION – VERSION 1.6 b) AADHAAR BEST FINGER DETECTION API SPECIFICATION – VERSION 1.6 c) AADHAAR E-KYC SPECIFICATION – VERSION 1.0 (FINAL) d) AADHAAR OTP REQUEST API SPECIFICATION – VERSION 1.6 e) AADHAAR MOBILE UPDATE API SPECIFICATION – VERSION 1.0	Mandatory
Reports & Additional Requirements		
1.	The Solution should be capable of sending alerts/SMS/email to predefined designated officers in the event of crossing predefined conditions.	Desirable
2.	The Solution should have Ability to generate reports at • real time / on line basis • in background (when evaluation is time-consuming) • via batch processing • specific date • regular time interval • any other specific business condition	Desirable
3.	Ability to maintain audit trail of changes such as the time of change, the user ID, old and new value with field description.	Desirable
4.	Ability to support the following functions: • Portability • Interoperability • Scalability • High Performance • Serviceability • Manageability • Flexibility	Mandatory
5.	All sensitive data (such as passwords, Aadhaar Data, bank account numbers, etc) shall have to be stored in encrypted format. The system should protect the integrity and authenticity of	Mandatory

	the data.	
6.	The solution must allow users to trace the history of a data. It should also be able to trace where a data entity currently is placed in the system.	Mandatory
7.	UIDAI/CIDR over a period of time may alter the metadata including the number of fields, data type etc. The system should be able to handle such situations	Mandatory
8.	The system should have provision for the user to submit the data through an easy to use interface like GUI, Web-Service, etc. as appropriate for the data exchange modes.	Mandatory
10.	The system should be able to support all standard file formats including but not limited to CVS, XML, XLS, Delimited File, rar, zip, 7z, jpg, jpeg etc.	Mandatory
11.	The solution should support bulk loading of data and inbuilt capability of data integration in near real time batch modes.	Mandatory
12.	The system should be able to match each record with the entire CIDR data through fuzzy logics to arrive at strict and lose matches.	Mandatory
13.	The system should also be able to make the match on various attributes including but not limited to name, date of birth, father's name, parsed address etc.	Mandatory
14.	The module should also ensure storage of any such data/logs which shall be required by Government, UIDAI and KSA/ASA. These logs shall support in creation of the compliance reports required by audit agencies.	Mandatory
15.	The system should be able to use the parsed data intelligently for the matching to take place. All possible permutations and combinations should be applied to arrive at the most probable match. The cutoff score should be definable for the 1:1 match (1 record of department matched with 1 record of CIDR) and the 1: N match (1 record of department matched with N records of CIDR). All the parameters should be configurable.	Mandatory
16.	The System shall have the capability of sharing data through common file sharing mechanism including FTP, Web-Service, etc.	Desirable
17.	The system should be flexible enough to accommodate the updates released by UIDAI from time to time without any additional cost.	
Special Requirements		
1.	The solution must have provision to sign and encrypt the authentication/e-KYC requests through digital signature certificate in High Availability mode.	Mandatory
2.	All requests and responses should be logged.	Mandatory
3.	The system shall maintain audit logs for all authentication, e-KYC, BFD related transactions by capturing desirable details of the transaction including Aadhaar number, date, time, IP, Sub-AUA code, Key, etc. AUA shall log all its authentication transactions and maintain them for at least 6 months' time period. The logs shall capture details of authentication	Mandatory

	transaction but not corresponding Personal Identity Information (PID).	
4.	The system should ensure that the authentication request originating at an authentication device is compliant with the standards and specifications prescribed by UIDAI and complete.	Mandatory
5.	The System should also be able to conduct Buffered Authentication (At places of poor network connectivity, authentication request may be "buffered" (or queued) on the device until a configurable period of time (presently 24 hours) then sent to CIDR for authentication when connectivity is restored / available)	Mandatory
6.	The system should be able to accept the e-KYC requests from KUA/sub KUA. System should be able to route the e-KYC request to KSA. The response from CIDR has to be forwarded to the KUA/sub KUA. (This may include the e-KYC information or the error code.). The same has to be given back to the sub organization in a secured manner. The application should validate the e-KYC request coming from KUA/Sub KUA and should digitally sign the packet. The system should decrypt the KYC details provided by CIDR and shall forward the KYC details including his name, address, photograph DoB, etc. to the clients in a secured manner. The system should have error handling facility.	Mandatory
7.	The Software solution must be compatible/inter-operable with various STQC Certified PoS (Point of Sale)/Wall-mount devices used for Finger print/IRIS scanning. Respective API to integrate these devices with software must be made available for fast implementation.	Mandatory
8.	Compliance of the security guidelines issued from time to time by Department of Telecommunications (DoT), government of India and UIDAI. Worker would be required to fulfill the all requirement of DOT & UIDAI in this respect.	Mandatory
9.	Any other requirement to fulfill the ASA and AUA scope work defined by UIDAI.	Mandatory
10.	Any other requirement to integrate with existing system of Customer for ASA and AUA services	Mandatory
11.	To provide required support to end customers for ASA and AUA services as per SLA	Mandatory
Disaster Recovery site		
1.	Disaster Recovery setup for Application for the ASA and AUA services	Mandatory
Billing Portal		
1.	Web based Billing portal should be part of the solution.	Mandatory
2.	Billing portal should have following features: 1. Separate login for customer, Railtel and MSP. There should be no limitation in creating the number of logins in the portal. 2. Customer should be able to view and download reports on the total number of transaction done by him. 3. The reporting should be available on various type of authentication methods like otp, ekyc, demographic, biometric etc. 4. The customer login of the billing portal should also contain the dashboard showing	Mandatory

	the billing statement on realtime basis. 5. Railtel/admin login should have feature for generating the transaction report and billing statement for all the customers based on the filter criteria like Customer name, date etc. The reports should be available for at least last 6 months. 6. Railtel/admin portal should allow for setting per unit transaction price for each customer.	
3.	Portal should have feature for sending email, sms etc. alerts to the customers/stakeholders.	Desirable

3.2 Proposed Responsibilities of MSP

a. Under the framework of the agreement, RailTel and MSP would work together towards a mutually beneficial relationship wherein MSP shall act as the deployment and implementation partner for the various projects undertaken or to be undertaken by RailTel during the term of the agreement for Aadhaar based Authentication and e-KYC services.
b. MSP shall provide their expertise in delivering the various solutions. These shall include but not limited to the following:
    i. Aadhaar based authentication for any financial / non-financial transactions that require authentication.
    ii. Aadhaar based Authentication during enrolment of Aadhaar enabled bank accounts. This service would also be used for financial transactions as per RBI guidelines.
    iii. Aadhaar based Authentication to verify the investor and transactions for insurance sector as per IRDA guidelines.
    iv. Aadhaar based Authentication for various Governments to Citizen (G2C) services envisaged to be provided through various agencies.
    v. Aadhaar based Authentication for skill development programs undertaken by various government agencies.
    vi. Aadhaar based Authentication during recruitment and other examinations.
    vii. Aadhaar based Authentication for monitoring attendance of various functionaries like school, office, factory, etc.
    viii. Aadhaar based Authentication for customer verification for mobile connections, LPG connections, etc.
    ix. Aadhaar based Authentication for train and any travel service where verification is required.
    x. e-KYC services for providing government centric services like passport service, election services, public distribution schemes, disbursements and other government initiated welfare schemes.
    xi. For any other purpose that may relate to Aadhaar enabled service delivery.
    xii. Aadhaar based Authentication for printing of Aadhaar cards, demographic updation, and biometric updation.
    xiii. For any other similar purposes that may envisage in future.
c. MSP shall provide their expertise in modification of the existing applications to be made suitable for Aadhaar enabled service delivery over RailTel / non-RailTel network.

d. MSP shall provide their support in procurement of equipment envisaged to be necessary for implementing the project.
e. RailTel shall procure the equipment necessary for implementation as per the existing guidelines.
f. MSP shall maintain requisite skilled manpower for Help Desk & L-1 Support, and, if found necessary for maintenance/support, the same shall be deployed as per request from RailTel. RailTel reserves the right to call the employees of MSP for a test or interview. RailTel also reserves the right to inspect the mark sheets/score cards, degree or certifications of such employees.
g. Training shall be imparted to RailTel technical team regarding the use of developed solution.

CHAPTER 4

Commercial Terms and Conditions

1. Service Level Agreement

The MSP should provide the comprehensive capability for management, maintenance and monitoring of all the overall Aadhaar Application Software Platform (including all components and sub-components) for this project. The SLA Monitoring function of the solution is an important requirement of this Project. Therefore, resolution of any issues/problems related to Aadhaar Application Software Platform is essential and unavoidable part of MSP responsibilities. If the MSP fails to resolve such an issue attributable to software within 48 hours of email/telephonic escalation/letter, under conditions of no law and order concerns to the satisfaction of RailTel, this may invoke penalty @ 1% per day of delay beyond 72 Hours, maximum up to Rs 10% of the monthly payment due to MSP.

2. Performance Bank Guarantee (Security Deposit)

2.1. The successful bidder shall have to submit a performance bank guarantee of 10% of the value of the LOA/PO within 30 (thirty) days from the issue of issue LOA/PO with validity upto 4 months beyond agreement period for the satisfactory performance of contract. Extension of time for submission of PG beyond 30 days and upto 60 days from the date of issue of LOA may be given by the authority who is competent to sign the contract agreement. However, a penal interest of 15% per annum shall be charged for the delay beyond 30 days i.e. from 31st day after the date of issue of LOA. In case the contractor fails to submit the requisite PBG even after 60 days from the date of issue of LOA, the contact shall be terminated duly forfeiting EMD and other dues, if any payable against the contract. The failed contractor shall be debarred from participating in re-tender for the work.

2.2. The Performa for PBG is given in Chapter 5, Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately

2.3. The security deposit/PBG shall be submitted to Corporate Office & will bear no interest

3. Agreement Details

The agreement shall come into effect from the date of signing and will be valid for a period of 1 year from the date of execution and shall be renewable for further terms as per mutual consent.

Termination of contract may also happen in case of below mentioned breach of SLAs:

1. If there is a breach in SLA from MSP side for two consecutive months, RailTel will analyze the problem and recommend measures to improve the same.
2. If still there is a breach in SLA from MSP side for the 3rd month, then a written notice that says "***If the service level is immediately not improved then the agreement is liable to terminated."*** will be issued to MSP by RailTel.
3. If the SLA still did not meet even in the 4th month, then Termination notice will be served from RailTel.

RailTel's decision shall be final in regard of Agreement renewal or termination.

4. Commercial Terms

The revenue shall be generated by way of Aadhaar enabled authentication and e-KYC services. RailTel shall charge its customers on per transaction basis and revenue is expected to be generated through these transactions. RailTel shall share with MSP a Fixed Percentage of its share of such revenue from all transactions that use Aadhaar enabled authentication and e-KYC services. The payment shall be made to MSP on quarterly basis. Details as under:

- Fixed MSP service revenue share = % of per transaction charges obtained by RailTel.

On expiry of the agreement period and issue of the certificate of final acceptance of the entire installations, the Performance Bank Guarantee shall be released to the Vendor after adjustment of any dues payable by the vendor.

5. RailTel's Responsibilities and Obligations

It shall be the responsibility of RailTel to create Network Infrastructure to support Aadhaar business. Following are the responsibilities of RailTel with respect to Network Infrastructure:

- RailTel shall provide & manage Network Infrastructure required to support Aadhaar business.
- Further RailTel shall also augment capacity and plan a resilient network to handle traffic as per business projections.
- RailTel shall provide 24x7 support at Network Operation Centre to facilitate rollout and support of network for Aadhaar Project.

6. Bid submission and Opening date

6.1. The bid should be submitted in single copy. The Envelope containing the bid should be sealed by the personal seal of the bidder. Each and every page of bid should be numbered and signed by authorized representative of the firm. Power or attorney in favour of the signatory duly authorizing the signatory shall be enclosed in the bid.

6.2. The envelope shall be addressed to the Purchaser at the following address:

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,

Sector-44, Gurgaon-122003

6.3. The envelope shall bear name of the work, the tender no. and the words "DO NOT OPEN BEFORE" (due date).

6.4. Offer / Bid should be delivered/submitted to the above address so as to reach up to 15:00 Hrs of due date. Tenders will be opened on specified date & time as mentioned in the tender in presence of such Tenderer'/ Representatives who choose to be present. Offers / Bids received after due date and time of submission shall be summarily rejected and shall not be opened.

In case the date of opening happens to be a holiday, the tender will be received and opened at the same time on the next working day.

7. Period of Validity

Offer shall remain valid for a period of 2 months from the date of opening of the bids

8. Clause wise Compliance

Clause wise compliance statement of the Terms & Conditions shall be enclosed with the offer along with the technical literature of the material and other documents in support of relevant clauses.

9. FORCE MAJEURE

Force majeure shall mean-

- War, hostilities (whether was be declared or not), invasion, act of foreign enemies.
- Rebellion, revolution, insurrection, or military or usurped power, or civil war.
- Ionizing radiation, or combination by radio activity from any nuclear fuel, or from any nuclear waste from the combustion of nuclear fuel, radio active toxic explosive or other hazardous properties of any explosive nuclear assembly or nuclear component thereof.
- Presume waves caused by aircraft or other aerial devices travelling at sonic or supersonic speeds.
- Riot, commotion or disorder, unless solely restricted to employees of the Contractor or of his subcontractors and arising from the conduct of the works.
- Loss or damage due to the use or occupation by the Employer of any section or part of the Permanent Works, except as may be provided for in the Contract.
- Loss or damage due to the extent that it is due to the design of the Works, other than any part of the design provided by the Contractor or for which the Contractor is responsible, and
- Any operation of the forces of nature against which an experienced contractor could not reasonably have been expected to take precautions.

10. Bid Earnest Money, Security deposit & tender document Fees

10.1. The bidder shall furnish a sum as Earnest Money in the form of Demand Draft from any scheduled bank in India in favor of "RailTel Corporation of India Limited" payable at New Delhi.

10.2. The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the order and fails to furnish performance bank guarantee (security deposit) in accordance with clause as mentioned in WORK.

10.3. Offers not accompanied with Earnest Money shall be summarily rejected.

10.4. Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible as but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

10.5. The successful bidder's EMD will be discharged upon the bidder's acceptance of the order satisfactorily and furnishing the performance bank guarantee in accordance with clause as mentioned in tender.

10.6. Earnest Money will bear no interest.

10.7. Bidder has to submit the bid earnest money of Rs. 2,400/- (Rs. Twenty four hundred Only) in the form of Demand Draft favoring RailTel Corporation of India Limited payable at New Delhi.

10.8. On receipt of the Letter of Acceptance from RailTel, the successful Worker shall within a period of 15 days deposit with RailTel an amount @ 10% of the value of order as Performance Guarantee for due fulfillment of the contract.

10.9. The Performance Guarantee should be valid for two months beyond the period of contract. The Performance Guarantee will be refunded or Bank Guarantee released to the vendor after adjustment of any dues payable by the vendor, two months after the expiry of the contract.

11. Late Bids

Any bid received by RailTel after the deadline for submission of bids will be rejected and/or returned unopened to the bidder, if so desired by RailTel.

12. Clarification

Recipients are required to direct all communications related to this tender, through the Nominated Point of Contact person:

Contact : Pawan Kumar Sharma
Position : Jt.GM/DN
Email : pawan@railtelindia.com
Phone No. : 971764497

13. Period of Agreement

RailTel will enter into an agreement with the bidder for a period of three year that can be extended mutually in steps of one year up to a maximum of 5 year total period.

14. Settlement of Disputes

In case of any dispute concerning this order both the Firm and RailTel shall try to settle the same amicably through mutual discussion/negotiations. Any unsettled dispute shall be settled in terms of Indian Act of Arbitration and conciliation 1996 or any amendment thereof.

Place of arbitration shall be New Delhi. Arbitrator shall be appointed by Managing Director, RailTel Corporation of India Limited.

15. Governing Laws

This contract shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

16. Termination for Default

RailTel may without prejudice to any other remedy for breach of contract, by written notice of default, sent to the supplier, terminate this contract in whole or in part if the firm fails to deliver services within the time period (s) specified in the contract.

17. Termination for Insolvency

RailTel may at any time terminate the contract by giving written notice to the firm, without Compensation to the firm, if the becomes bankrupt or otherwise insolvent as declared by the Competent court provided that such termination will not prejudice or affect to the RailTel.

18. Rates during Negotiation

The tenderer/s shall not increase his/their quoted rates including payment terms in case the RailTel Administration negotiates for reduction of rates. Such negotiations shall not amount to cancellation or withdrawal of the original offer and the rates originally quoted will be binding on the tenderer/s

19. Bill passing & Paying Authority

Accounting unit/bill passing unit for the supplies under SOR is GGM/DNM/CO. Bills to be submitted to the GGM/DNM for payment.

20. Wrong Information by Tenderer

If the tenderer/s deliberately gives/give wrong information in his/their tender which Creates/create circumstances for the acceptance of his/their tender the RailTel reserves the right to reject such tender at any stage.

21. Security Considerations & Security Agreement

The directives issued from time to time by the Department of Telecommunications (DoT), Ministry of Communications and IT or any other Ministry of Govt. of India on security considerations shall be applicable to the present tender. Accordingly, as per the extent amendment of the National Long

Distance (NLD) Service License Agreement for Security related concerns for expansion of Telecom Services in various zones of the country issued vide Department of Telecommunication, Ministry of Communication and IT, Govt. of India's letter no. 10-54/2010-CS-III (NLD) dated: 31.05.2011, you shall comply with the provisions stated in the above mentioned directive of DoT and shall have to enter into an agreement with RailTel as per the mutual agreement between Telecom Service Provider and the vendor of equipment, product and services (based on template, available on DoT website) covering all relevant clauses. You must submit a declaration along with their bid in this regard

22. Limitation of Liability

Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

(a) the Supplier shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser; and

(b) the aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Purchaser with respect to intellectual property rights infringement.

****

CHAPTER-5

Form No. 1

Performa for Performance Bank Guarantee

PERFORMANCE BANK GURANTEE BOND

(On Stamp Paper of Rs One Hundred)

(To be used by approved Scheduled Banks)

1. In consideration of the RailTel Corporation of India Limited : Sector-44,Plot No.143, Gurgaon-122003(Herein after called RailTel) having agreed to exempt …….. (Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Agreement No. …… …… dated …… made between …… and …….. for (hereinafter called "the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, or production of a Bank Guarantee for Rs. …….. (Rs…….. only). We, ……(indicate the name of the Bank) hereinafter referred to as " the Bank") at the request of ……. ……. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs. ……. Against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, ……. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. ……

3. We, …….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Supplier(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal.
The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Supplier(s) shall have no claim against us for making such payment.

We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the

said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……. (1) ……. We shall be discharged from all liability under this Guarantee thereafter.

We, ……. (indicate the name of Bank) Further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) Supplier(s).

(indicate the name of Bank) lastly undertaken not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

Dated the day of 2016

for ……..

(indicate the name of the Bank)

Witness

1. Signature
   Name

2. Signature
   Name