AUA/KUA Booklet

AUA/KUA On Boarding & Technical Documents – Version 1.0

October 2016

CENTRE FOR e-GOVERNANCE
e-Enabling Government

Center for e-Governance

TABLE OF CONTENTS

Sl No	Content	Page no	Version
1	AUA On Boarding Process Summary	1	-
2	AUA Handbook	5	1.0
3	Elligibility Criteria for On Boardinng AUA/KUA	27	1.0
4	AUA Application Form	40	1.4
5	UIDAI-AUA Agreement Template	44	-
6	ASA-AUA Agreement guidelines	59	1.0
7	AUA-SUB AUA Agreement guidelines	61	1.0
8	AADHAAR OTP Request API	63	1.6
9	AADHAAR Authentication API Specifications	69	2.0
10	AUA Audit Compliance Check List	87	-
11	AUA Go Live Check List	89	-
12	AADHAAR eKYC Services	90	-
13	KUA On Boarding process	99	0.4
14	KYC User Agency Application form	106	-
15	KUA Go Live Check List	107	1.0
16	AADHAAR E-KYC API Specification	108	2.0
17	AADHAAR Authentication Standards & Specifications	116	1.7
18	Creating a circle of Trust- AADHAAR Authentication Services A Strategy Paper	118	-
19	UIDAI Biometric Device Specifications(Authentication)	124	-
20	Biometric Authentication Devices -Single Finger Capture	126	2.1.2
21	Biometric Authentication Devices -iris	139	2.1
22	Resident consent Form	141	-
23	Contact Details	142	

AUA On boarding Process Summary

The below engagement process is intended to provide the interlock points between UIDAI and probable AUAs, and to briefly describe the common steps for adopting Aadhaar based business model. Please note that this section outlines the steps for a regular engagement with an Organization. The order of steps could potentially vary on case to case basis depending on the understanding of an organization and the support required by the organization to adopt Aadhaar based business model. Moreover to reduce the cycle time of the onboarding process, some of the activities could be carried in parallel depending on the requirements and capability of the organization.

Step 1: Application Enquiry (By AUA): An organization interested in becoming an Authentication User Agency (AUA) sends a request to enquire about the authentication services offered by UIDAI and to understand the process for getting access to Authentication services. Organizations (prospective AUAs) could send their requests to UIDAI for getting access to information on Authentication Services through: Authentication ecosystem management support email: auth.ecosys@uidai.gov.in

Step 2: Responds to AUA enquiry (By UIDAI): UIDAI sends a suitable response to organization enquiry, share AUA related documentation and proposes to conduct a kick off session on the Authentication services. UIDAI team shares the contact details of the team managing the organization engagement and provides access to Authentication Services knowledgebase which includes the documents like AUA Handbook, AUA Application form, UIDAI-AUA Agreement, List of Supporting documents, Guidelines.

Step 3: Submits application with supporting documentation (By AUA): Organization submits the application with supporting documents as per the eligibility criteria provided in Aadhaar Authentication Operating Model and organization type as specified in the List of support documents and application process.

Step 4: Verifies and approves application (By UIDAI): UIDAI engagement team scrutinizes the AUA application and supporting documents as per the guidelines and specifications of Aadhaar Authentication Operating Model, List of support documents and application process and other documents published by UIDAI from time to time. UIDAI team will approve the application and inform the entity.

Step 5: Signs agreement (By UIDAI & AUA): At this stage, an AUA is expected to understand the UIDAI. Authentication services and agree to fulfill the requirements as per UIDAI specifications including setting up infrastructure and aligning business process applications to the Aadhaar Authentication application. Once both AUA and UIDAI are satisfied, they proceed to sign an agreement. UIDAI and AUA enter into an agreement as per the UIDAI-AUA Agreement.

Note: At this step an AUA is also expected to have an arrangement in place with an UIDAI approved ASA to access UIDAI authentication services as explained in above section 2.0 of this document. An arrangement with an ASA is required by an AUA to get access to UIDAI Authentication database (CIDR). An AUA may enter into an agreement with an ASA as deemed appropriate by the two parties. To provide support on the agreement, UIDAI has published Guidelines for AUA ASA Agreement.

Step 6: Need support for readiness (By UIDAI): Based on interaction during the previous steps of the process and inputs from an AUA, UIDAI engagement team assesses the level of support to be provided for go live readiness. In majority of the cases the assessment for the level of support required by an AUA is accomplished in collaboration with an ASA. An ASA plays a vital role in onboarding and readiness of an AUA as the connectivity between AUA and ASA is a pre-requisite for an AUA to access Aadhaar authentication services. If the readiness support assessment outcome is **Yes** , please go to step 7. Else, please go to step 8.

Step 7: Conduct onboarding workshop in collaboration with an approved ASA (By UIDAI): UIDAI team engages with an approved ASA to define the schedule and agenda of onboarding workshop and shares it with prospective AUA. Both UIDAI and ASA provide access to preparation material on Aadhaar Authentication services to better prepare an AUA for the workshop.

Step 8: Build Infrastructure and Submits Request for Pre-Production Access to ASA (By AUA): AUA builds the required infrastructure for adopting Aadhaar authentication with support provided by UIDAI engagement team and through the below mentioned mediums:

- UIDAI Authentication Application Developer Portal https://groups.google.com/forum/#!forum/aadhaarauth
- UIDAI empanelled consultants
- Authentication API
- OneTimePIN (OTP) API
- Best Finger Detection API
- Technology FAQs

If using Biometric authentication, AUA is required to procure and deploy certified devices as per Biometric Devices Specifications for Aadhaar Authentication. For process of device certification and list of certified suppliers and biometric devices (Authentication), please refer STQC website at http://stqc.gov.in/content/bio-metric-devices-testing-and-certification. Once the required infrastructure for Aadhaar authentication is ready and arrangements with an UIDAI approved ASA is in place, AUA will request the engaged ASA to send the request for pre-production environment access.

Step 9: Facilitate Readiness and Submits Request for Pre-Production Access (By ASA): ASA facilitates AUAs technical readiness and subsequently send the request for pre-production

environment access to UIDAI authentication support team at authsupport@uidai.gov.in asking for the AUA code and license key.

Step 10: Assist in Preproduction Integration and Execution in collaboration with an approved ASA (By UIDAI): UIDAI authentication support team in consultation with an ASA provides access to pre-production environment and enables the AUA to establish end to end connectivity through an ASA server to carry out authentication services testing. UIDAI Authentication support team responds to pre -production access request received from ASA by sharing the AUA code and license key to enable AUA to conduct end to end testing. At this stage an AUA is also linked with an approved ASA in the UIDAI backend system which enables the ASA and UIDAI to process authentication transactions transmitted by an AUA.

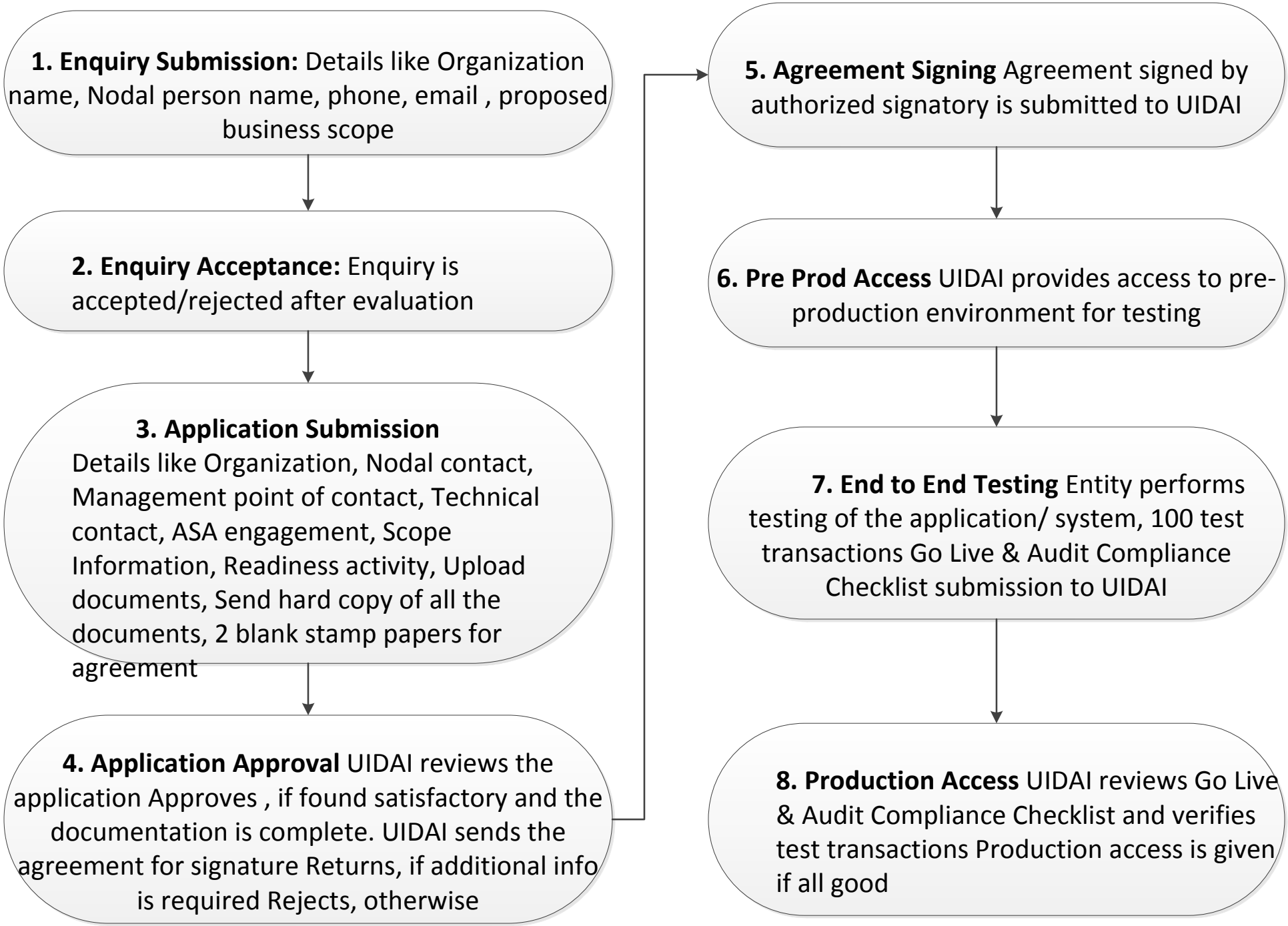
Step 11: Conducts End to End testing with an approved ASA, Audit and Submits Request for Go Live (By AUA): AUA engages the respective ASA and conducts end to end testing on UIDAI pre-production environment. Post successful end to end testing AUA engages an Auditor to conduct the compliance audit as per Aadhaar Authentication Standards and Specifications. Subsequently AUA completes the go live checklist and submits the request for go live with the following documents:

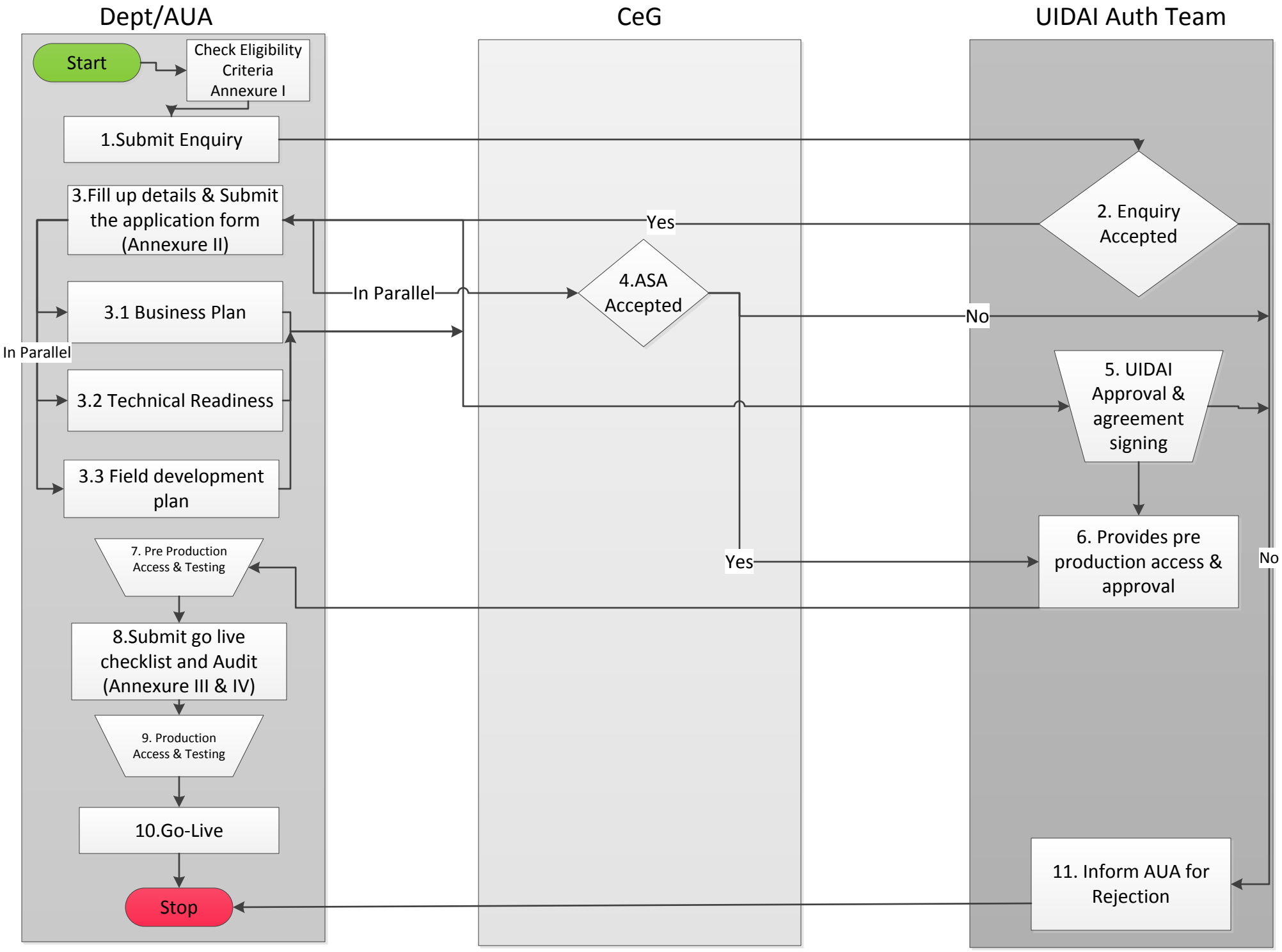
- Go Live checklist (Provided as part of the AUA Application form).
- Audit certificate as proof of compliance to current UIDAI standards and specifications.

Step 12: Approve and assist in Go Live (UIDAI): UIDAI engagement team scrutinizes the AUA go live request as per the Go-Live checklist and supporting documentation and seeks internal approvals for Go Live. UIDAI provides access to AUA authentication admin portal for accessing AUA code and License Key.

Step 13: Production release and operations management (By AUA): AUA establishes a production release and operations management mechanism. Note: For any Technical Operations Support for live AUA, please contact UIDAI by sending an email to authsupport@uidai.gov.in or by calling at 011-23462644.

Flowchart for AUA On-boarding Process




Dept/AUA
CeG
UIDAI Auth Team
Start
Check Eligibility Criteria Annexure I
1.Submit Enquiry
2. Enquiry Accepted
3.Fill up details & Submit the application form (Annexure II)
Yes
In Parallel
4.ASA Accepted
3.1 Business Plan
No
In Parallel
5. UIDAI Approval & agreement signing
3.2 Technical Readiness
3.3 Field development plan
6. Provides pre production access & approval
Yes
No
7. Pre Production Access & Testing
8.Submit go live checklist and Audit (Annexure III & IV)
9. Production Access & Testing
10.Go-Live
11. Inform AUA for Rejection
Stop

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

AADHAAR AUTHENTICATION USER AGENCY (AUA) HANDBOOK - Version 1.0

January 2014

1 Table of Contents

2 Introduction 4
3 Authentication Services Overview 4
4 AUA Operating Model at a Glance 6
5 AUA-UIDAI Engagement Process 8
6 Steps for Implementing Aadhaar Authentication 13
6.1 Initiation 13
6.1.1 Aadhaar Based Business Model 14
6.1.2 Technology Roadmap 14
6.2 Readiness 14
6.2.1 Define Aadhaar Enabled Processes 14
6.2.2 Technology Infrastructure 18
6.3 Implementation 21
6.3.1 Aadhaar Enabled Process Development 21
6.3.2 AUA Server and Device Applications 22
6.3.3 AUA Server Application Architecture 22
6.3.4 Setup Environment 24
6.3.5 AUA Applications 25
6.3.6 Best Finger Detection (BFD) Application 25
6.3.7 Finger Print Authentication Application 29
6.3.8 IRIS Authentication Application 31
6.4 Compliance 34
6.4.1 Audit 34
6.4.2 Testing 35
6.5 Roll out 36
6.5.1 Go Live and Training 36
6.5.2 Release and Operate 37
7 Suggestions to Improve Authentication Success Rate 38
7.1 Reasons of True rejects and ways to avoid the same 38
7.2 Recommendations 38
7.3 Best Practices 40
8 Appendix 42
8.1 Related Publications/ Tools 42
8.2 Glossary of Terms and abbreviations 43

Table of Figures

Figure 1: Authentication Service Overview 5
Figure 2: Transaction Flow of Aadhaar Authentication Process 7
Figure 3: AUA On-boarding Process 8
Figure 4: Aadhaar Implementation Stages 13
Figure 5: Illustrative High Level Architecture of AUA Server 23
Figure 6: BFD Capture Process (1-10 Fingers) 26
Figure 7: BFD implementation Sample Screens for a Point of Sale/ Micro ATM Based application 26
Figure 8: BFD Sample Screen for a Computer Based Application (1) 27
Figure 9: Sample Screen for a Computer Based Application (2) 27
Figure 10: Authentication Process Flow 32
Figure 11: IRIS Capture Image 32
Figure 12: Indicative Deployment Architecture 37

2 Introduction

This Authentication User Agency (AUA) handbook is the administrative handbook which should be referenced for integrating with UIDAI as an Authentication User Agency (AUA) to consume or offer authentication services for resident service delivery. The purpose of this document is to outline the UIDAI and AUA Engagement process, the technical design of AUA Applications and network, and provide information on how to Leverage Aadhaar based authentication system in various service delivery applications.

This document is not intended to address specific low level details of the actual engagement and implementation of AUA applications due to the wide range of domain specific applications. This document will help AUAs in Aadhaar Authentication based solution implementation and ensuring necessary business and technical compliance.

The intended audiences for this document are AUAs stakeholders (Business and Technology Teams), the project development teams and technical architects. For the technology part, the reader is assumed to have knowledge in network administration, web services development and deployment, system security and architecture with good level of experience in software development.

General good practices like project management, resource engagement, general security, hardware setup etc. are not included, AUAs are expected to leverage their existing project implementation processes and take own judgment for such cases. However Authentication best practices, based on Quality of service study done on ongoing pilot projects, are included in this document.

This document will be updated and refined regularly to incorporate the feedback from stakeholders especially existing AUAs.

3 Authentication Services Overview

The purpose of Authentication is to enable Aadhaar-holders to prove their identity and for service providers to confirm the resident's identity claim in order to provide services and give access to benefits. Aadhaar Authentication shall make life simpler for the resident as it is meant to be a convenient system to prove one's identity without having to provide identity proof documents whenever a resident seeks a service.

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data such as biometric/demographic information is submitted to UIDAI (Central Identities Data Repository-CIDR) for matching, following which the UIDAI verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. UIDAI confirms either proof of identity or verifies the information provided by the resident based on the data available at the time of Authentication. To protect resident's privacy, Aadhaar authentication service responds only with a "**Yes / No**" and no Personal Identity Information (PII) is returned as part of the response.

Aadhaar Authentication enable residents to prove their identity based on the biometric and /or demographic information, thus making the process of identification convenient and accurate.

Aadhaar Authentication system supports the following Authentication types:

1. Biometric Matching

a. Finger Print Authentication
b. IRIS Authentication

2. Demographic Matching
3. Additional features such as One-Time-PIN (OTP)

Biometric Matching

Biometric Matching refers to the usage of Aadhaar Authentication for matching the biometric attributes (Finger Prints or IRIS) of a resident in the UIDAI database (CIDR) to the biometric data submitted by the resident on an authentication device and return the response in Yes (Successful Authentication) and No (Failed Authentication).

Demographic Matching

Demographic matching refers to the usage of Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, gender, etc. as per API specifications) of a resident in the UIDAI database (CIDR) with the data in the AUA's database or with demographic data submitted at the point of authentication and return the response in Yes (Successful Authentication) and No (Failed Authentication).

One-Time-Pin

In case of matching using One-Time-PIN (OTP) an OTP is sent to the registered mobile number of the resident seeking Aadhaar Authentication. The OTP shall have a limited validity of 15 min. The resident shall provide this OTP during authentication and the same shall be matched with the OTP at the UIDAI CIDR. Same process is following in case of PIN based authentication, where a PIN submitted by the resident is matched against the PIN in CIDR and returns the response in Yes (Successful Authentication) and No (Failed Authentication).

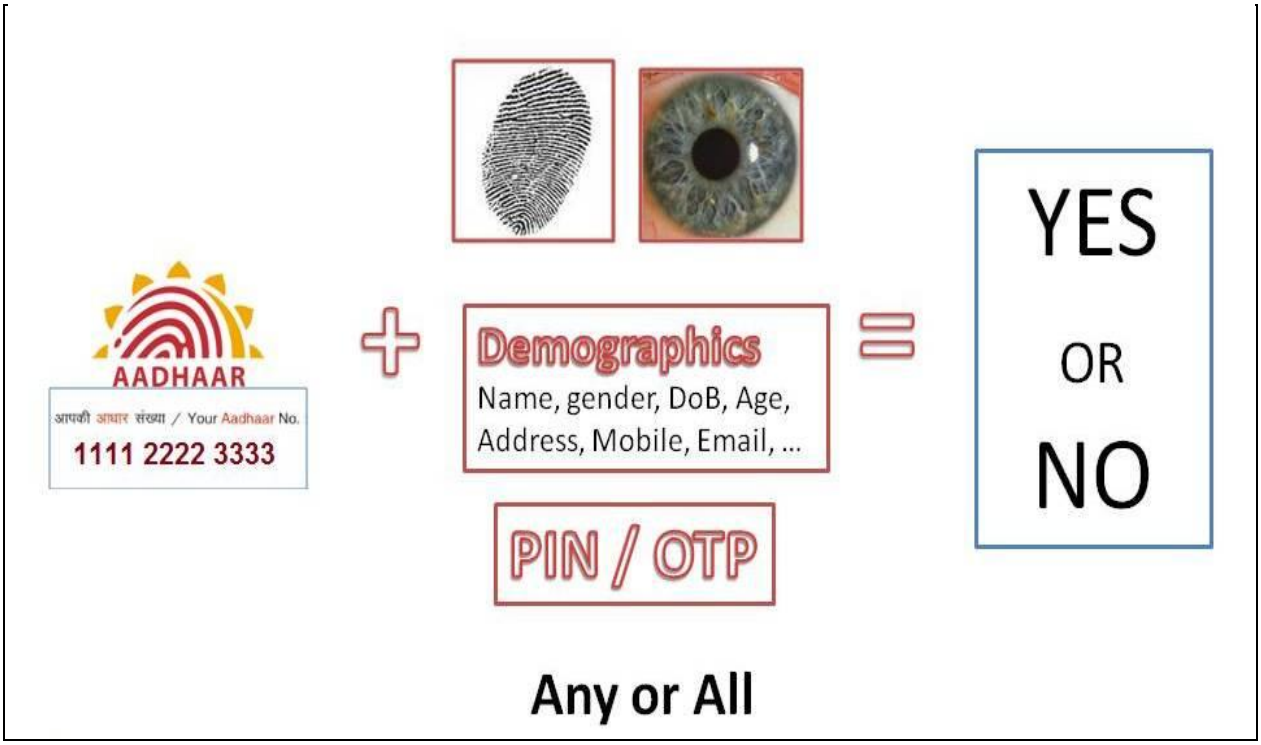


Figure 1: Authentication Service Overview

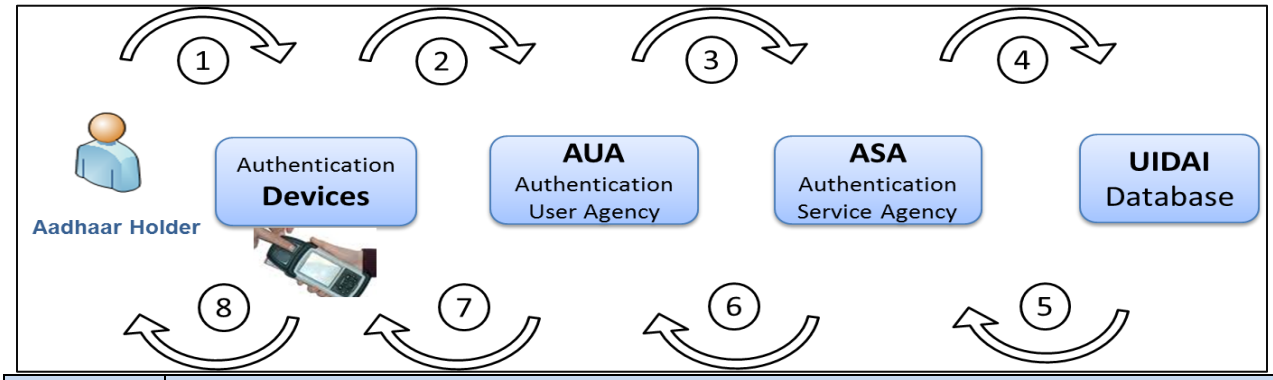
4 AUA Operating Model at a Glance

As a part of authentication services roll-out strategy, UIDAI engages with Authentication User Agencies (AUAs - who would deliver services to their beneficiaries by using Aadhaar based model for verification) and Authentication Service Agencies (ASAs). Below table explains in detail about AUA/ASA and other important actors in Aadhaar Authentication eco system.

Aadhaar Authentication Operating Model Actors	Definition
Aadhaar Holder	These are holders of valid Aadhaar numbers who seek to authenticate their identity towards gaining access to the services offered by the AUA or their Sub-AUAs.
Authentication Devices	These are the devices that collect personal identity data (PID) from Aadhaar holders, prepare the information for transmission, transmit the authentication packets for authentication and receive the authentication results. They could be operator-assisted devices or self-operated devices. Examples of authentication devices include desktop PCs, laptops, kiosks, handheld mobile devices (microATMs),IRIS devices etc.
Authentication User Agency (AUA)	AUAs are agencies that use Aadhaar authentication to enable its services and connects to the CIDR by itself (as an ASA) or through an existing third party ASA. It is also possible that an AUA engages more than one ASA. In order to directly connect to the CIDR, an AUA needs UIDAI's approval to become an ASA. An AUA could also transmit authentication requests from other entities that are "Sub AUAs" under it (see details on Sub AUA below).AUAs can also act as an aggregator offering authentication services to Sub-AUAs below them and may also offer value added services such as multi-party authentication, MIS reports and authorization to their Sub AUAs.
Sub AUA	Sub AUAs are agencies that use Aadhaar authentication to enable its services through an existing AUA e.g. IT Department of a State Government could become an AUA and other departments in the State would access Aadhaar authentication services through the IT Department as its Sub AUAs.
Authentication Service Agency (ASA)	ASAs are agencies that have established secure leased line connectivity with the UIDAI Database (CIDR) in compliance with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (see below for description of AUA) and transmit AUAs' authentication requests to CIDR. An ASA could serve several AUAs; and may also offer value added services such as multi-party authentication, authorization and MIS reports to AUAs.
UIDAI	UIDAI is the overall regulator and overseer of the Aadhaar authentication system. It also owns and manages, either by itself or through an agency, the UIDAI Central Identities Data Repository (CIDR) that contains the personal identity information / data of all Aadhaar-holders.

The below diagram provides an illustrative transaction flow of a service delivery request originated by an Aadhaar holder using an authentication device which is processed through the AUA, ASA and UIDAI channel:

Figure 2: Transaction Flow of Aadhaar Authentication Process



Process Step	Description
1	An Aadhaar Holder resident approaches a Service delivery point (e.g. PDS shop, a banking correspondent) and originates the service request by using the authentication devices (e.g. hand held devices – MicroATM). Alternatively, a service provider may approach the resident for Aadhaar authentication. (E.g. LPG delivery boy coming to a household for LPG delivery with a biometric authentication device).
2	An Authentication device processes the request by collecting the Aadhaar number and the demographic, biometrics (Finger prints and/or IRIS) and/or OTP if required of the resident, and subsequently sends the request to an UIDAI server. Authentication devices are deployed on the service delivery points either by the AUAs directly or through their business partners (e.g. Banking Correspondents).
3	AUA processes the request as per the standards and specifications of the partner ASA and UIDAI. AUAs have the option of partnering with multiple ASAs to connect with UIDAI database for verification of the residents.
4	ASA receives the requests from an AUA as per the specifications of UIDAI and sends the packet to UIDAI database for verification.
5	UIDAI processes the request and provides "**Yes** / **No**" response to ASA.
6	ASA compiles the response from UIDAI and sends the same to AUA in agreed format.
7	AUA processes the service request based on the response received from ASA and sends the response to authentication device for processing the service request.
8	Authentication device processes the response from AUA and delivers the service as per the business instructions received from an AUA.

Please refer UIDAI website at http://uidai.gov.in/auth.html for more details on below topics of Aadhaar Authentication Operating Model

- Introduction to Aadhaar authentication service
- Engagement model: roles, responsibilities and obligations of key actors
- Variation of the engagement model: buffered authentication

5 AUA-UIDAI Engagement Process

Onboarding Process

The below engagement process is intended to provide the interlock points between UIDAI and probable AUAs, and to briefly describe the common steps for adopting Aadhaar based business model. Please note that this section outlines the steps for a regular engagement with an Organization. The order of steps could potentially vary on case to case basis depending on the understanding of an organization and the support required by the organization to adopt Aadhaar based business model. Moreover to reduce the cycle time of the onboarding process, some of the activities could be carried in parallel depending on the requirements and capability of the organization.

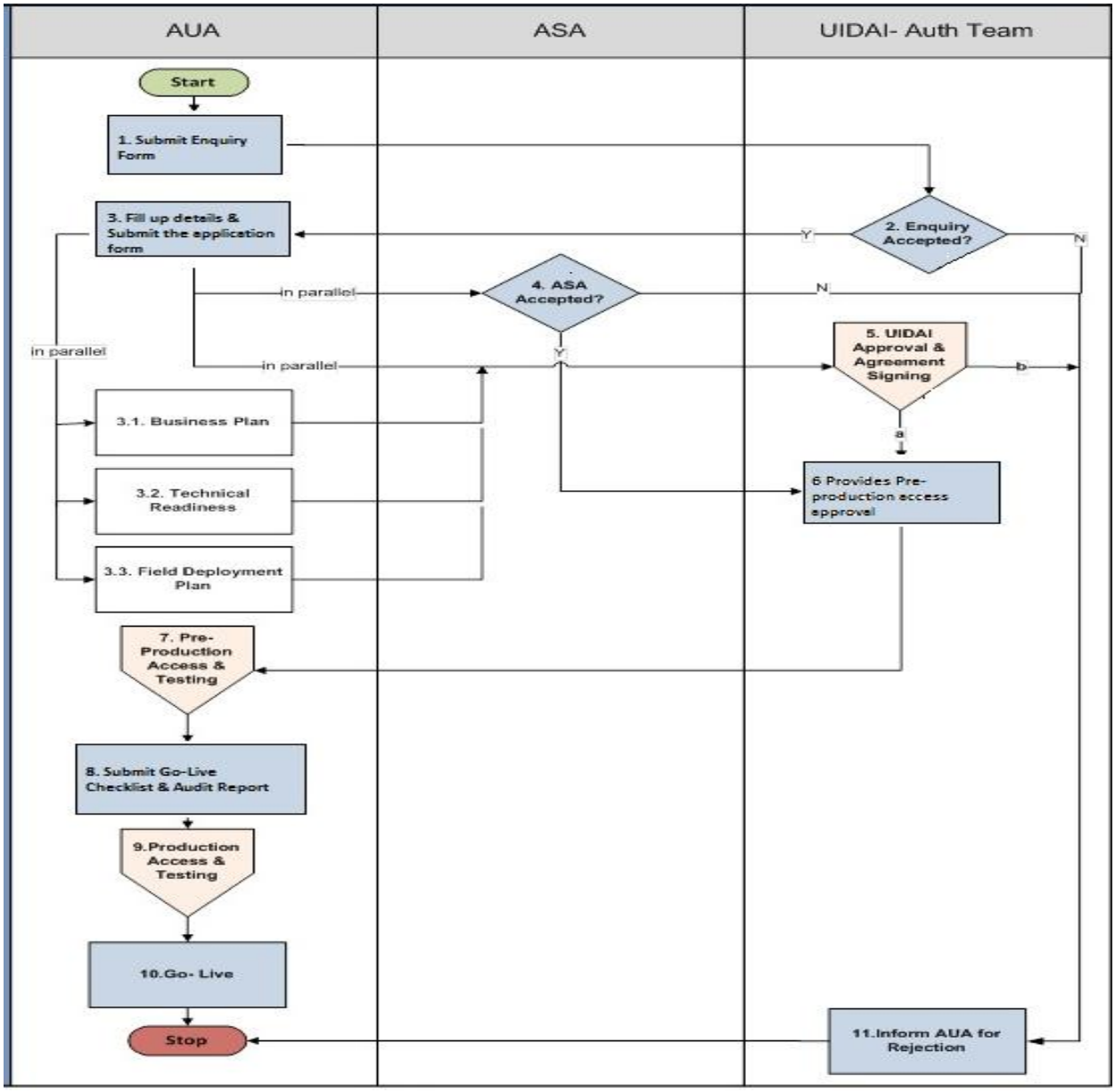


Figure 3: AUA On-boarding Process

Step No.	Step Description	Actor(s)	Functional Description
1.0	Application Enquiry	AUA	An organization interested in becoming an Authentication User Agency (AUA) sends a request to enquire about the authentication services offered by UIDAI and to understand the process for getting access to Authentication services. Organizations (prospective AUAs) could send their requests to UIDAI for getting access to information on Authentication Services through: • Authentication ecosystem management support email auth.ecosys@uidai.gov.in • Letter to UIDAI Authentication Team at Headquarters or 8 Regional Offices • Authentication portal
2.0	Responds to AUA enquiry	UIDAI	UIDAI sends a suitable response to organization enquiry, share AUA related documentation and proposes to conduct a kick off session on the Authentication services. UIDAI team shares the contact details of the team managing the organization engagement and provides access to Authentication Services knowledgebase which includes the documents listed below: • Aadhaar Authentication Operating Model • AUA handbook • AUA Application form • UIDAI-AUA Agreement • List of support documents and application process • Guidelines for AUA-ASA Agreement • List of current ASAs **Note:** Above document names are hyperlinks. Complete URLs are also provided in Appendix 5.1.
3.0	Submits application with supporting documentation	AUA	Organization submits the application with supporting documents as per the eligibility criteria provided in section 2.4.2 of Aadhaar Authentication Operating Model and organization type as specified in section 2.0 of List of support documents and application process (and other documents published by UIDAI from time to time. The information of these documents will be provided to an AUA in step 2.0.
4.0	Verifies and approves application	UIDAI	UIDAI engagement team scrutinizes the AUA application and supporting documents as per the guidelines and specifications of Aadhaar Authentication Operating Model, List of support documents and application process and other documents published by UIDAI from time to time. UIDAI team will approve the application and inform the entity.

Step No.	Step Description	Actor(s)	Functional Description
5.0	Signs agreement	UIDAI and AUA	At this stage, an AUA is expected to understand the UIDAI authentication services and agree to fulfill the requirements as per UIDAI specifications including setting up infrastructure and aligning business process applications to the Aadhaar Authentication application. Once both AUA and UIDAI are satisfied, they proceed to sign an agreement. UIDAI and AUA enter into an agreement as per the UIDAI-AUA Agreement. **Note**: At this step an AUA is also expected to have an arrangement in place with an UIDAI approved ASA to access UIDAI authentication services as explained in above section 2.0 of this document. An arrangement with an ASA is required by an AUA to get access to UIDAI Authentication database (CIDR). An AUA may enter into an agreement with an ASA as deemed appropriate by the two parties. To provide support on the agreement, UIDAI has published Guidelines for AUA-ASA Agreement.
6.0	Need support for readiness?	UIDAI	Based on interaction during the previous steps of the process and inputs from an AUA, UIDAI engagement team assesses the level of support to be provided for go live readiness. In majority of the cases the assessment for the level of support required by an AUA is accomplished in collaboration with an ASA. An ASA plays a vital role in onboarding and readiness of an AUA as the connectivity between AUA and ASA is a pre-requisite for an AUA to access Aadhaar authentication services. If the readiness support assessment outcome is "**Yes**", please go to step 7. Else, please go to step 8.
7.0	Conduct onboarding workshop in collaboration with an approved ASA	UIDAI	UIDAI team engages with an approved ASA to define the schedule and agenda of onboarding workshop and shares it with prospective AUA. Both UIDAI and ASA provide access to preparation material on Aadhaar Authentication services to better prepare an AUA for the workshop.
8.0	Build Infrastructure and Submits Request for Pre-Production Access to ASA	AUA	AUA builds the required infrastructure for adopting Aadhaar authentication with support provided by UIDAI engagement team and through the below mentioned mediums: • UIDAI Authentication Application Developer Portal • https://groups.google.com/forum/#!forum/aadhaarauth • UIDAI empanelled consultants • Authentication API • OneTimePIN (OTP) API

Step No.	Step Description	Actor(s)	Functional Description
			• Best Finger Detection API • Technology FAQs If using Biometric authentication, AUA is required to procure and deploy certified devices as per Biometric Devices Specifications for Aadhaar Authentication. For process of device certification and list of certified suppliers and bio-metric devices (Authentication), please refer STQC website at http://stqc.gov.in/content/bio-metric-devices-testing-and-certification. Once the required infrastructure for Aadhaar authentication is ready and arrangements with an UIDAI approved ASA is in place, AUA will request the engaged ASA to send the request for pre-production environment access. .
9.0	Facilitate Readiness and Submits Request for Pre-Production Access	ASA	ASA facilitates AUAs technical readiness and subsequently send the request for pre-production environment access to UIDAI authentication support team at authsupport@uidai.gov.in asking for the AUA code and license key.
10.0	Assist in Pre-production Integration and Execution in collaboration with an approved ASA	UIDAI	UIDAI authentication support team in consultation with an ASA provides access to pre-production environment and enables the AUA to establish end to end connectivity through an ASA server to carry out authentication services testing. UIDAI Authentication support team responds to pre -production access request received from ASA by sharing the AUA code and license key to enable AUA to conduct end to end testing. At this stage an AUA is also linked with an approved ASA in the UIDAI backend system which enables the ASA and UIDAI to process authentication transactions transmitted by an AUA.
11.0	Conducts End to End Testing with an approved ASA, Audit and Submits Request for Go Live	AUA	AUA engages the respective ASA and conducts end to end testing on UIDAI pre-production environment. Post successful end to end testing AUA engages an Auditor to conduct the compliance audit as per Aadhaar Authentication Standards and Specifications. Subsequently AUA completes the go live checklist and submits the request for go live with the following documents: • Go Live checklist (Provided as part of the AUA Application form).

Step No.	Step Description	Actor(s)	Functional Description
			• Audit certificate as proof of compliance to current UIDAI standards and specifications.
12.0	Approve and assist in Go Live	UIDAI	UIDAI engagement team scrutinizes the AUA go live request as per the Go-Live checklist and supporting documentation and seeks internal approvals for Go Live. UIDAI provides access to AUA authentication admin portal for accessing AUA code and License Key.
13.0	Production release and operations management	AUA	AUA establishes a production release and operations management mechanism. Note: For any Technical Operations Support for live AUA, please contact UIDAI by sending an email to authsupport@uidai.gov.in or by calling at: 011-23462644.

6 Steps for Implementing Aadhaar Authentication

Implementing Aadhaar authentication for service delivery has a lot of similarity with a typical business and IT project based on Software Development Life Cycle (SDLC) with standard stages as Analyze, Design, Develop, Test, Implement and Operate.

The diagram below represents a consolidated view of the sections of this handbook that outlines the illustrative stages involved in implementing Aadhaar based model for service delivery, and the roles played by business and technology teams. Please note that the detailed steps in each of the implementation stages outlined in this section are illustrative and could potentially vary on case to case basis depending on the capability and team structure of an AUA for adopting the Aadhaar based business model.

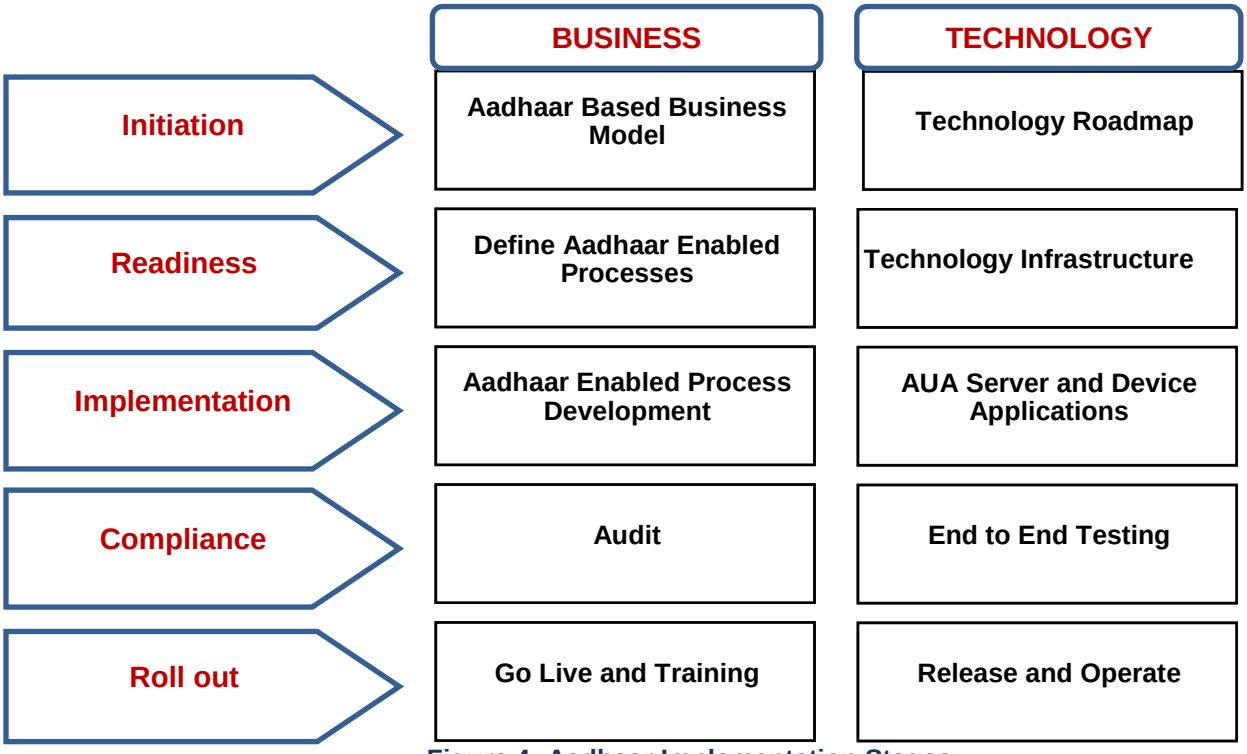


Figure 4: Aadhaar Implementation Stages

6.1 Initiation

This is the first stage where an organization, interested in becoming an AUA, initiates the process of incorporating Aadhaar authentication in their business model for services delivery.

Key steps at this stage are listed below:

- Definition of Aadhaar Based Business Model
- Definition of Technology Roadmap

Outcome of this stage would be a well-defined implementation roadmap with activities and stakeholders (Internal and External Teams) responsibilities from Day1 of project implementation to Go-live.

6.1.1 Aadhaar Based Business Model

A well - defined plan for integration of Aadhaar into AUA business solution for service delivery is critical for harnessing value from Aadhaar authentication. AUAs are expected to start with the step of building an understanding of the functionality offered by Aadhaar authentication and thereof analyze the business direction to define the Aadhaar implementation scope.

Key business model milestones should include the following:

- Formation of a Joint Working Group (with members from AUA Business and Technology Team, ASA Business and Technology Team, UIDAI, Authentication device vendors etc.)
- Identification of business areas for Aadhaar implementation
- Selection of domain specific process for pilot implementation
- Linking of Aadhaar into selected business process
- Definition of roll out strategy including selection of pilot geographies based on the Aadhaar penetration i.e. areas with high % of Aadhaar enrolments
- Definition of process for procurement of certified authentication devices
- Definition of audit and security specifications
- Definition of training requirements

6.1.2 Technology Roadmap

In this stage AUA defines the key technology milestones as part of the business project plan for implementation of Aadhaar based solution. An AUA is expected to identify the core team based on the understanding of Aadhaar Authentication for laying out the implementation plan with defined delivery milestones.

Key technology milestones should include:

- Identification of technology team to form a part of the Joint Working Group
- Procurement of hardware and software
- Environment setup
- End to end Connectivity with ASA and other business partners (e.g. Sub-AUA, if any)
- Server application design and development
- Device applications design and development
- End to end testing with UIDAI pre-production environment
- Implementation of MIS and fraud monitoring
- End to end testing with UIDAI production environment before roll out of the service to end customers Production Release
- Operations Management

6.2 Readiness

6.2.1 Define Aadhaar Enabled Processes

To integrate Aadhaar, an AUA needs to analyze the As-Is business processes for identifying the business areas where Aadhaar Authentication based service delivery could be adopted.

To successfully implement this, an AUA needs to focus on various aspects, especially:

1. To - Be domain specific processes
2. Linking Aadhaar with existing Resident ID (Also referred to as Aadhaar Seeding)
3. Ensuring Inclusion and taking measures to avoid service disruption (Also referred as Exception Handling)
4. Fraud Monitoring

To - Be Domain Specific Processes

AUA would be required to define the to-be processes for service delivery. Key aspects of the to-be processes are:

- Analyze As-Is process and process challenges
- Identify processes which can be modified to leverage the benefits of Aadhaar Platform (For example: ID Verification)
- Analyze Service Delivery Data to understand the data structure differences across silos, formats in which data exists
- Analyze the way data is shared among various process owners during service delivery
- Identify common data model required for service delivery
- Definition of the business rules for acceptance of Aadhaar based authentication for service delivery e.g.
    - Rules for cleansing the resident/beneficiary databases through the process of Aadhaar linking. E.g. During the process if there are more than 1 record having similar name and address with different resident IDs, all the residents are required to physically report and may also be required to give biometric details for Aadhaar mapping.
    - Rules for processing of the authentication request and handle the response for service delivery etc.

Linking Aadhaar with Existing Resident ID (Also Referred to as Aadhaar Seeding)

Delivery of services through Aadhaar based authentication is dependent on linking of the Aadhaar number with existing Resident ID e.g. for direct transfer of government subsidy to a beneficiary will require mapping of Aadhaar number with the scheme entitlement ID and the bank account number of the beneficiary resident. The objective is not to replace the currently used unique identifier of the customers/ residents/ beneficiaries with Aadhaar but the objective is to seamlessly enable Aadhaar authentication without impacting any other interface that the service providers maintain with their customers.

Therefore, Aadhaar seeding is one of the most critical steps of the business readiness stage that could be achieved through a combination of several strategies, as no single solution will apply to all cases. It is essential that every seeding process is thoroughly analyzed and planned before proceeding with actual seeding. While it is the responsibility of the service providers to seed their service delivery databases with Aadhaar, UIDAI will support by providing sample tools, best practices and consulting advisory on request.

Primarily there are two ways of seeding of service delivery database with Aadhaar number:

	Description	Example	UIDAI Sample Tools
1. Top-Down method	This is a method using which Service Delivery data records are matched with Aadhaar enrollment data (KYR/KYR+/EID-UID) in order to find a suitable match. Upon finding a match, Aadhaar	1. MGNREGA Job Card number was captured as KYR+ field at the time of the enrolment. The fields Job Card Number and Resident name can then be used along with UID number available from EID-UID XML files to find a matching unique record in MGNREGA database.	State Resident Data Hub (SRDH) – Batch Seeding Module for State Governments. Ginger - a tool built

	Description	Example	UIDAI Sample Tools
	number is seeded into the service delivery database. Exact match or best match strategies may be used in this case.	2. A combination of various fields from Service Delivery database records is matched with SRDH records to get the best matches, and a verifier may select the right record/UID for seeding.	internally at UIDAI
2. Bottom-up method	This involves creation of touch points with the residents where the residents voluntarily or in response to service provider's call initiates inclusion of their UID in service delivery databases.	1. A department can leverage one or more channels of communication with the residents in order to capture their Aadhaar numbers e.g. Document collection camps where Residents are expected to hand over copies of Aadhaar letter and registration form with the service provider (ex. Ration card). Service provider later updates the service delivery database based on the information supplied.	SRDH - Manual Seeding Module

Please refer UIDAI website at http://uidai.gov.in/images/aadhaar_seeding_v_10_280312.pdf for more details on below topics on Aadhaar Seeding:

- Aadhaar Seeding Strategy
- Why Aadhaar seeding is required
- Pre-requisites of Aadhaar Seeding
- Seeding categories
- Common challenges
- Case studies (with sample Oil and Marketing Companies and Banks Approach)
- UIDAI seeding utility- Ginger

Ensure Inclusion and Avoid Service Disruption

In any identity verification program it is important to decide what exception rate is acceptable and how to handle the exception cases for 100% inclusion of the residents for service delivery. Like any other technology, biometrics based authentication has certain limitations. There will always be a set of population who will not be able to (temporarily or permanently) authenticate through biometric authentication system due to multiple reasons, such as:

- Residents with missing biometric characteristics; for example, no fingers
- Residents engaged in hard manual labor (such as construction, mine workers) having all of their fingers in extremely poor condition with respect to fingerprint quality
- Residents having illness such as cataract problem, burnt/cut fingers
- Extreme environmental conditions with direct sunlight, high humidity and dryness
- Very young (children) and very elderly population having undefined features, soft and wrinkled skin

To ensure that such genuine residents are not denied service delivery, and the existing service delivery is not interrupted by introduction of Aadhaar based solution, an AUA would require exception handling process i.e. usage of alternative ways of verifying the residents for service delivery. UIDAI recommends implementing a multi factor authentication (also known as Federated Authentication) where Aadhaar authentication can be used in conjunction

with AUAs domain/application specific authentication schemes. Some solutions could be using alternate biometric modalities, allowing multiple attempts, operator authentication, using demographic / OTP based authentication etc. Adopting federated model is also expected to aid handling of biometric exceptions.

Some examples of the exception handling process are listed below:

- One of the banks has advised its Banking Correspondents (BCs) to keep withdrawal slips at the point of service delivery. Genuine residents who do not succeed in biometric authentication are asked to fill up the withdrawal slip and sign/give thumbprint. The withdrawal slip is then countersigned by the Mukhiya / local representative. On his next visit to bank branch, the BC gets cash from the bank and hands over to the resident.
- The Food &Civil Supplies Department of a State Government has recorded mobile numbers of all its beneficiaries (almost 98% have mobile phones). In case of biometric failure, a One-Time-PIN (OTP) is sent to the recorded mobile number and authentication is done basis OTP success. This OTP is different from the OTP authentication offered by UIDAI. For the remaining 2% residents, manual authentication is done through existing ration card of the resident.

Besides biometric limitations, there could also be occasional network challenges. Online authentication essentially requires network connectivity. For cases where connectivity is intermittent or connectivity is a little distance away, UIDAI proposes a solution called “buffered” authentication wherein authentication request may be “buffered” (or queued) on the device until a pre-specified period of time, which is currently 24 hours, and then sent to CIDR for authentication when connectivity is restored / available.

Note: The exception handling mechanisms should be backed up by reliable features to log and track requests handled through exception handling mechanism to prevent any fraud attempts.

Fraud monitoring

One of the key benefits foreseen of Aadhaar authentication is elimination of ghosts and fakes and ensuring that services are delivered to the right beneficiaries. However, as explained in point 3 of this section, due to limitations of biometric authentication, AUAs need to deploy exception handling mechanism. This in turn could lead to potential misuse of exception handling mechanism to divert services to other parties and deny services to actual beneficiaries.

AUAs that currently face problems of diversion of services/goods to non-deserving parties especially need to ensure that the exception handling mechanism is backed by a fraud monitoring mechanism.

In order to avoid security issues, inconvenience to resident and to streamline the process for exception cases, it is strongly recommended that the authentication application should have an option to record these cases along with AUA/operator details for better reporting, analysis and traceability. The number of manual override/exception handling attempts should be tracked and only limited number of manual overrides could be allowed per day per terminal to prevent operator malpractice.

An example of fraud monitoring working in tandem with exception handling is as follows. An LPG delivery organization that uses biometric authentication (but allows for manual overrides in case of biometric rejects) requires the operator to log into the system before start of service delivery through secure credentials. Upon observing high biometric reject rates, it started analyzing biometric reject percentages by delivery boy. Certain delivery boys appeared to have much higher reject rates than others. When this feedback was given to the respective dealers and data closely monitored, the manual overrides / biometric reject rates came within acceptable limits.

6.2.2 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. AUAs are required to create their own actual requirements based on services they plan to offer, choice of technology, and existing resources within their IT system.

Hardware to be provisioned by AUA is listed below:

- It is recommended that AUA has a lease line or a dedicated connectivity with ASA network.
- Bandwidth requirements should be computed based on the expected volume of transactions from Sub AUAs/Devices.
    - Roughly about 5K average bandwidth is required for each API call.
    - Handling about 1 Lakh transaction per hour requires about 28 transactions per second (tps) on an average. Considering 30-40% spike, bandwidth for about 40 tps needs to be planned for. This turns out to be around 1.6 Mbps (40*5K*8 bits/sec).
    - AUAs may start with a 1 Mbps link and expand as volumes increase.
- Within AUA Network
    - Network equipment's – appropriate network equipment's to connect from Sub AUAs/Devices and further to ASA.
    - One server (dual quad-core blade/rack servers with 64 GB RAM) with cluster setup having two or more nodes or at least 2 servers (dual quad-core blade/rack servers with 32 GB RAM recommended) for hosting AUA server within AUA data center in an active-active (preferred) or active-standby mode. Server sizing needs to be done by AUA based on actual AUA server performance and expected volumes.
    - HSM Box is recommended to protect digital signature and to handle large volume digital signing.
    - Firewall server – for securing network from Sub AUA to AUA and then AUA to ASA. It is suggested that two different firewall products from two different vendors be deployed for better security. AUAs could use existing firewalls in their network for this purpose. There is no requirement for a dedicated firewall.
    - Other security appliances/servers – In addition to firewall, it is recommended that AUAs provision for network intrusion detection and prevention systems as well as anti-virus and anti-malware systems to ensure AUA network is protected from attacks.
    - If auditing is done using a database, at least 2 servers to install and configure audit database. To avoid audit database becoming a single point of failure, it is recommended that database be configured in active-active or active-standby mode.
    - Storage required for maintaining audits for at least 6 months. Considering 5K audit size per transaction, for 10 Lakh transactions a day, ASAs require 5GB of storage size. If AUAs retain audit logs online for, say, 1 month, then 150GB online storage is required per month beyond which it could be moved to tape.

- 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.

    Some possible form factors in which biometric authentication devices may be deployed include the devices listed in the below table:

Hand-Held / PoS Device such as MicroATMs	
USB device connected to PC	
Mobile phone with biometric sensor	

Kiosks such as ATMs	
IRIS Device	
Mobile Phone	

Software to be provisioned by AUA is listed below:

- Server class Operating System for all machines deployed.
- Class II-III Digital Signature. For details on procurement, please read latest API documentation.
- AUA server software as described in the AUA Server Architecture section. AUA server functionality could be built using off-the-shelf open-source/commercial tools.
- Firewall software – it is suggested that, when using multiple firewalls, AUAs use products from different vendors to strengthen security. AUAs can choose to use existing firewalls within their IT system for this purpose.
- Database software (if auditing is database based) – if auditing is done in an RDBMS, then database software is required. AUAs can choose any open-source/commercial database based on their preference.
- Monitoring software to effectively monitor production system. Any enterprise monitoring software (EMS) could be used. AUAs can choose a commercial/open-source tool based on their preference or use an existing one that may be already in place within AUA IT system.
- Other related software tools for managing network devices, servers, and database, backup, replication, reporting tools for MIS purposes, integration to billing software for AUAs to bill Sub AUAs/device vendors.

Manpower to be provisioned by an AUA is listed below:

AUAs are responsible for all the devices, servers, and the network until the ASA network. If AUAs are offering 24 x 7 service availability to their Sub AUAs/devices, then network needs to be monitored and managed using people in multiple shifts. Appropriate team needs to be put in place to handle operations, security, and support to their AUAs to ensure high quality of service.

Key resources within AUA organization are listed below:

- Network administrators
- System administrators
- Database administrators

- Backup administrators
- Security administrators
- L1/L2/L3 support team
- Operations and Project Management team

6.3 Implementation

6.3.1 Aadhaar Enabled Process Development

At this stage AUA implements the Aadhaar enabled processes by deriving inputs from the readiness stage where the to-be processes are defined. In most of the cases an AUA would be engaging Business, IT teams and the Consultants / Software Solution Providers for development of the processes.

An AUA is expected to develop processes to manage the Aadhaar based authentication for service delivery in lines of process areas explained in the readiness section. So an AUA would ensure the development of applications for:

1. To be domain specific processes
2. Linking Aadhaar with existing Resident ID (Also referred as Aadhaar Seeding)
3. Ensuring Inclusion and avoid service disruption (Also referred as Exception Handling)
4. Fraud Monitoring

One of the key and mandatory areas of process development is Resident onboarding, where in business processes are put in place for information, education and communication of the residents availing services through Aadhaar based authentication. AUAs are expected to develop applications for helping the residents to understand the changes in service delivery process due to integration of Aadhaar Authentication in their business models e.g. need for the resident to link his Aadhaar number with the existing resident ID's, relevance of Aadhaar number and existing IDs / proofs of the resident. AUAs are required to develop processes for building and managing teams (service delivery operators) who would be interacting with residents. The resident onboarding process should also focus on Do's and Don'ts of Aadhaar authentication for both service delivery operators and residents.

To assist AUAs in developing processes to implement Aadhaar based authentication, UIDAI has published reference material that would provide assistance to AUAs while interacting with residents and also better enable the AUAs to inform and educate the residents about their biometrics and authentication process. The reference material is available at UIDAI website accessible at www.uidai.gov.in/auth and UIDAI developer portal accessible at https://developer.uidai.gov.in/site/home.

UIDAI also provides assistance to ecosystem partners for development of processes and applications through:

- UIDAI's empanelled Consultants and Software Solution Providers to provide assistance to potential AUAs.
    - Consultant would provide services on Process Reengineering, Project Management and Implementation support to AUAs for facilitating integration of their processes with Aadhaar.
    - Software Solution Providers would help in designing Aadhaar enabled Applications.

      For details please refer
      http://uidai.gov.in/images/FrontPageUpdates/final_empanelment_list_30_may_2011.pdf

- ICT Assistance

- ICT Assistance is provided to States for engagement of consultants and service providers for defining and developing Aadhaar applications

- UIDAI Support Team and Tools

  - Team will facilitate conceptualization and defining areas of Aadhaar usage jointly with AUAs and provide assistance in identifying applications solutions and necessary linkages.

6.3.2 AUA Server and Device Applications

AUAs can offer "Sub AUA/device application" multiple protocols and options for connecting their solution to Aadhaar system via ASA.

At a basic level, AUA services are:

- Preparing Auth request based on the latest API published by UIDAI using inputs from Sub AUA/devices (uid, tid, sa, data, hmac etc).
- Digitally Signing Authentication request
- Routing Authentication Request to ASA
- Receiving response from ASA and forwarding the same to Sub AUA/device.

In most of the cases AUA will be a service providing agency like a bank. So AUA server application development will be part of their business application development. There will still be few cases where AUA will only provide pure authentication services. It is advisable that in both the cases AUA server application is built separately and used as a service. AUA server application should have broadly following components/services:

- Validation component to validate input received from Sub AUA/Devices to prepare Auth request correctly.
- An auditing component to store request/response/failure and other key information like uid, tid, auth request date time, auth response date time etc. for auditing purposes.
- An independent component for digital signing of authentication request
- A component for MIS and Fraud Monitoring to generate various reports for stakeholders (UIDAI, ASA, Sub-AUA etc.) and monitoring service quality. This will also help in preventing misuse of services.
- An Authentication/Best Finger Detection (BFD) etc. message creator component to form request messages.
- An AUA request/response handler to handle request receive from Sub-AUA / Devices and response received from ASA.

AUA need to expose services (Web service recommended) to Sub AUAs /devices to place auth request to CIDR through ASA. Network connectivity between Sub AUAs /devices to AUA server can be through Internet, GPRS, and Broadband etc. in a reliable and secure fashion.

6.3.3 AUA Server Application Architecture

Following diagram depicts a high level architecture of an AUA server:

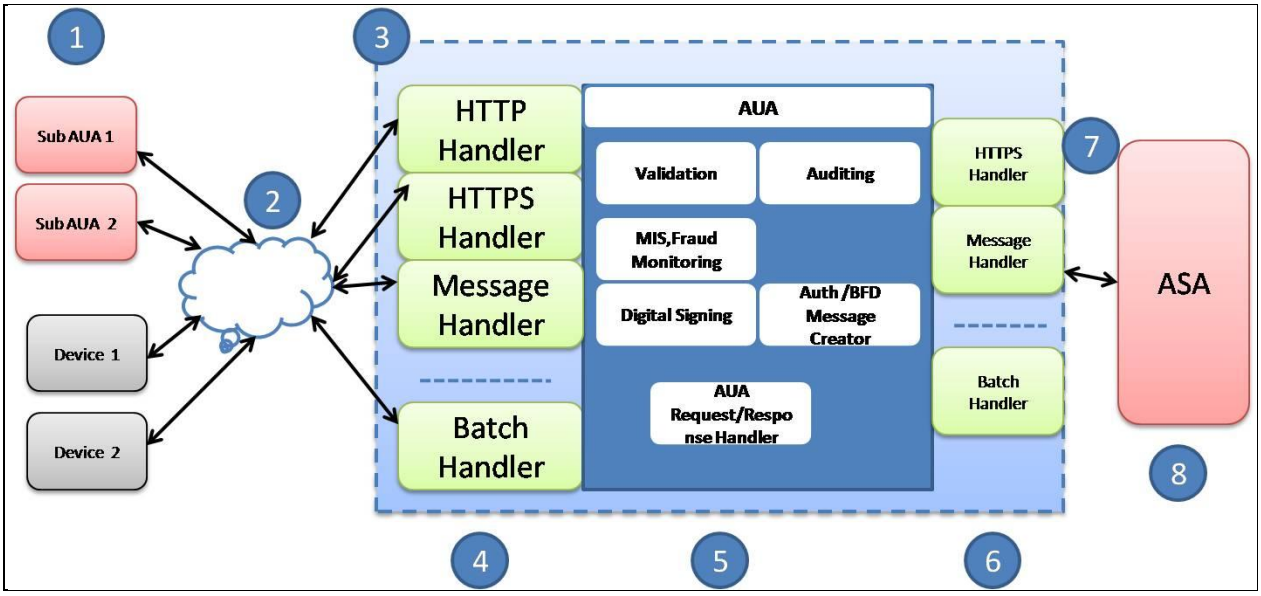


Figure 5: Illustrative High Level Architecture of AUA Server

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
    a. Network connectivity from devices to AUA server (Internet, GPRS, Broadband etc) in a reliable, secure fashion.
    b. Communication protocol can be the choice of AUA and Sub-AUA. Indicative options are mentioned in the diagram above (Figure 1).
    c. To make communication more secure VPN option could also be used.(suggested option in case of a Sub AUA)
3. AUA server (depicted in the light blue box with dotted line border)
    a. 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.
    b. 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:

4. If AUAs wishes to offer multiple choices in terms of how Sub AUAs/devices actually communicate with AUA server, it is suggested that, a well-designed layer handling various protocols be built.
    a. A pluggable set of protocol handlers could provide standard protocols such as HTTPS, JMS, etc. to be used for incoming communication from Sub AUAs/devices.
    b. Generic AUA application can provide wide range of data format (XML, binary formats such as ISO-8583 in the case of financial transactions, JSON, csv, etc.) to fulfill need of various kind of Sub AUA/devices.
5. Once the data is received in the AUA server, server needs to do the following:

a. Validate the input data to ensure compliance to Aadhaar data definitions as well as to eliminate issues such as SQL-injection etc.
b. After validation, format it to an XML format complying with Aadhaar API specifications.
c. Sign it digitally
d. Forward to ASA using appropriate protocol supported by ASA.
e. Audit Transaction into an audit database.
f. Format back response xml and send back to Sub AUA/Device specific format using an appropriate protocol adapter.

6. Network between AUAs and ASA.

a. This could be any kind of secure network depending on the needs of AUAs.
b. UIDAI suggests that this be a private leased line to have better control of availability, bandwidth, reliability, and security.
c. UIDAI mandates that communication between AUAs and ASAs for sending Aadhaar API requests and responses be secure.
d. Choice of specific protocol and security standards depends on the domain and application AUAs and ASAs are using.
e. Based on the application needs of AUA, API requests could be sent using a synchronous protocol (such as HTTPS) or an asynchronous protocol (such as a message queue).
f. For AUAs who are new and starting afresh, UIDAI suggests using HTTPS over a leased line to communicate between AUA and ASA.

6.3.4 Setup Environment

It is recommended that an AUA should have separate environments for development, testing and production.

UIDAI provides support to AUAs at all three stages for development, testing and production in line with the below table:

	Development	Pre-production	Production
Prerequisite to access UIDAI environments	No prerequisites- All prospective AUA can access the UIDAI development environment	UIDAI-AUA Agreement & Established connectivity with an UIDAI approved ASA having leased line connectivity with UIDAI in place.	Approval on UIDAI Go Live checklist and supporting documents
Support from UIDAI	•API's and Technical FAQs •UIDAI Developer portal with details of AUA Handbook, Sample code, Vanilla Applications etc. •Google group for technical and application queries.	•List of approved ASAs with contact details •Facilitates end to end testing with CIDR once ASAs provide staging test AUA code and license key to AUAs •Google group for technical queries	Provides AUA code and license key post Go Live approval

6.3.5 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:

1. Best Finger Detection Application
2. Finger Print Authentication application
3. IRIS Authentication Application
4. OTP

6.3.6 Best Finger Detection (BFD) Application

Best finger detection (BFD) application will determine the best fingers of the resident by analysing all the ten fingers of the resident. Recent studies have indicated that for most of residents, best fingers have higher probability of authenticating successfully in least number of attempts. As a result of the BFD, the residents are informed about their two best fingers (Rank 1 and Rank 2) which could be used for successful authentication. BFD is done only once before the first biometric authentication (irrespective of which AUA). If a resident forgets best fingers, he/she can still try authentication with other fingers (non-best fingers) or can request the AUA for BFD again.

Key benefits of BFD:

- Provide consistent higher authentication accuracy.
- Best finger detection improves reliability of authentication.
- Identify resident who are likely to need two fingers for authentication.
- Identify residents who may need to update their biometrics.
- Identify residents who may need to use alternate authentication mechanisms due to inherent poor finger quality.

BFD finger capture process

The following section outlines, the process of finger captures in order to determine best fingers. The same is outlined in Figure 6.

1. Capture one finger at a time in order specified in Figure 6.
2. One at a time, capture ten fingers. Ensure labelling is properly done. As a best practice following order is suggested Left little, Left Ring, Left middle, Left index, Left thumb, Right Thumb, Right index, Right middle, Right ring and Right little fingers in that order (refer Figure 6).
3. While capturing any finger, its NFIQ should be displayed in the client application.
4. Once the best attempt is captured for all fingers, application forms the input for the BFD API as specified in the Aadhaar Best Finger Detection (BFD) API 1.6.
5. Application invokes the BFD API through AUA server (similar to authentication process).

6. Based on the response, provide a printed receipt to the resident indicating the best fingers of the resident.
7. Once best fingers are detected among ten fingers, resident proceeds to conduct authentication thereon using the best fingers.In case, best fingers are not detected even after providing all 10 fingers, resident can attempt the process again or follow the error codes to take appropriate action as per the AUA guidance.

Figure 6: BFD Capture Process (1-10 Fingers)

Figure 7: BFD implementation Sample Screens for a Point of Sale/ Micro ATM Based application

Figure 8: BFD Sample Screen for a Computer Based Application (1)

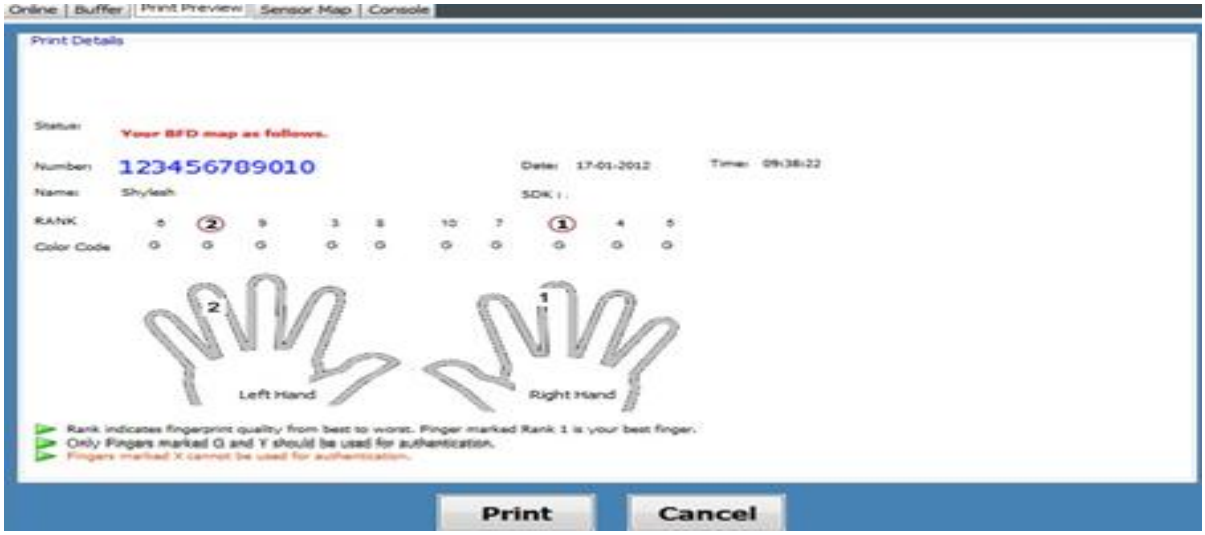


Figure 9: Sample Screen for a Computer Based Application (2)

Result of BFD Application

BFD server at UIDAI end processes incoming requests to look for best fingers among incoming fingers. Best finger process is expected to indicate all good fingers apart from best fingers as well as indicate suggested actions in case no good fingers are found. BFD application feedback helps resident to clearly identify which of his/her fingers are good for authentication. Resident is expected to use his/her fingers in the order of rank for authentication.

The BFD Application must be able to distinguish between a finger which was not sent for BFD and finger which was found to be of poor quality.

- Return code-“00”- Successful. Resident’s two best fingers indicated with indicated with rank1 and 2 so no further action is needed. Other fingers which can also be used for authentication is ranked in ascending order. Fingers not ranked **cannot** be used for authentication.

- Return code - “01”- No best finger found - Fingerprint quality of resident good. Check if Aadhaar number if entered correctly. Repeat BFD by paying attention to order of finger scanned. If Aadhaar was entered correctly, sequence of fingers scanned was right, then, biometric update will be needed for the resident through Aadhaar update process.
- Return code - “03”- No best fingers found. Check if Aadhaar number if entered correctly. Repeat BFD by paying attention to order of finger scanned. If Aadhaar was entered correctly, sequence of fingers scanned was right, then one possibility is resident fingerprint quality is very poor for authentication. Resident may obtain authentication results with very low reliability.
- Return code – “04”- Biometrics are not present in gallery, and user should go for re-enrolment.
- Return code - “99”- Biometrics related to Aadhaar number is not present in authentication database and is being populated. Try after some time. If the error persists, please refer to error code in the CONSOLE and report to technical support.
- For all other failure scenarios, “99” is returned - “Server cannot determine what action you should take, please look at the error code and see what needs to be done”. The error code, like in Authentication, will provide the context for what has happened on the server. For example, if error code was 510 – Invalid XML, the action is to fix the application code. Report the error code to technical support. Try repeating the test.

Actionable feedback message in English in case resident or operator needs to take specific actions. BFD applications should display message to enable operator and resident take appropriate actions.

BFD tool implementation

Authentication devices using biometric authentication implementing this BFD API should have the user interface for capture and sending as described below:

- Operator is expected to examine all ten fingers of the resident.
    - In case, fingers are excessively dry, wipe with wet cloth
    - In case, excessively wet, wipe it dry
    - In case, if fingers are not clean (dust/oil/grease), operator can request resident to clean the fingers.
- Resident/operator needs to clearly know which finger to capture and should be visible on screen.
- Operator should ask resident to keep finger on the device until its get appeared on the client app screen. Operator should also make sure that there would be a green light blinks on device while capture the fingerprints.
- There must be options to rescan after the capture is complete.
- Capture high quality fingers up to 3 attempts and application must pick up highest NFIQ image (if possible NFIQ 1 & 2).
- Application should remember the finger position because it has to be sent alongside NFIQ for every finger as part of BFD API input.
- Application must do local matching to avoid same finger being sent against different positions and to also ensure same finger is indeed used during multiple attempts.
- Application should send only templates and not images.
- Provide for exception where resident may not have all ten fingers. This can be achieved by providing skip flag for every finger. Operator can mark either mark fingers as skip or not scan/label.
- Provide an option to buffer the transaction in case the connectivity is not there and replay from database.
- Application must not store any unencrypted data that involves resident information including biometrics.

- BFD application must provide a printed receipt UI indicating BFD output details preferably with a picture of the hand
- Buffered/online transaction receipt needs to be provided to resident.
- Receipt needs to indicate rank as per response for each response and any action code/messages, if any.

6.3.7 Finger Print Authentication Application

In accordance with the API, authentication application on the MicroATM can package single finger or two finger minutiae records in the same transaction. Syntax for packing single or two finger minutiae records is elaborated in the Aadhaar Authentication API Specification.

Application is expected to implement two finger authentications as part of the fingerprint authentication module.

In the event of online Aadhaar authentication transaction, flow of events for carrying out two finger authentication is as follows.

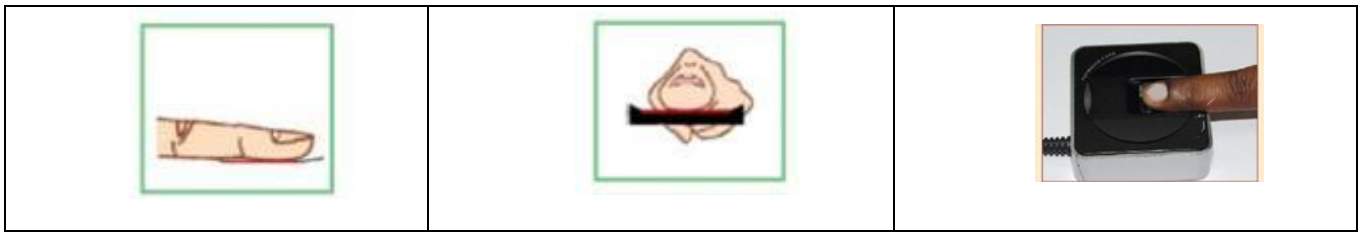
- After capturing the first best finger, the minutiae record is sent to UIDAI. A copy of the minutiae record for the first finger is retained in memory (as against stored on disk). This is single finger authentication.
- If the authentication transaction is successful, then the minutiae record is deleted from memory and application proceeds to next stage post authentication.
- If the authentication transaction is unsuccessful, then resident is requested to provide second best finger and minutiae record from first finger (retrieved from memory) as well as minutiae record from second best finger is submitted for two-finger authentication.

This completes one attempt of two finger authentication cycle. If the two finger authentication is unsuccessful, the same process can be repeated in order to enable successful authentication.

Finger print authentication process

- Operator is expected to examine fingers of the resident.
    - In case, fingers are excessively dry, wipe with wet cloth
    - In case, excessively wet, wipe it dry
    - In case, if fingers are not clean (dust/oil/grease), operator can request resident to clean the fingers.
- Displaying the number of minutiae points captured and NFIQ of image (when possible) helps operator to improve the quality of the image capture.
- Quality checking software (NFIQ) can be implemented on the device helps measure quality of capture. Capture high quality fingers up to 3 attempts and application can highest NFIQ image to enable more reliable authentication. (If possible, prefer NFIQ 1 & 2). NFIQ computation is expected to take more than 5 seconds on existing MicroATM implementations. Hence computing NFIQ is not mandatory and other means to provide quality feedback such as number of minutiae in the captured sample can be explored.
- Operator should ensure that for the residents BFD have already done. In case residents have not done the BFD, the operator should do BFD first. Please refer section 5.2.3.2 to see the BFD process.
- Improving authentication reliability by providing feedback regarding capture quality – Submitting minutiae records with less number of minutiae points' risks unsuccessful authentication. Headers of ISO minutiae record provide information related to number of minutiae points. When less than 20 minutiae points are captured, operator should capture once again in order to increase the number of minutiae points. Up to three capture attempts can be conducted in order to increase the minutiae points in the captured image.
- In case of connectivity issues, two fingers can be captured at once and two finger authentication transactions can be carried out in buffered mode.

- During multiple attempts, simplified two finger scheme can be implemented which is detailed below. By retaining the last captured fingerprint minutiae in memory, application can only request one best finger and form two finger authentication requests. Sample capture flow process is indicated below.
    - Capture 1 – 1st best finger – single finger auth transaction
    - If fail, Capture 2 – 2nd best finger – two finger auth transaction (using capture 1 and 2)
    - If fail, Capture 3 – 1st best finger – two finger auth transaction (using capture 2 and 3)
    - If fail, Capture 4 – 2nd best finger – two finger auth transaction (using capture 3 and 4)
- This flow helps resident to achieve authentication in minimal number of captures.
- Application must not store any unencrypted data that involves resident information including biometrics.
- Resident is expected to place the finger on the sensor platen in the figure below. Resident is expected to place the finger as straight as possible and should be able to apply mild pressure to enable good quality capture. Sensors must be mounted on the device in order to enable good quality capture both in table top mode as well as handheld mode.



- Figure below indicates improper ways to for resident to place finger on the sensor.
- Devices can integrate the prompts on the screen (where picture display is possible) indicating best ways to place fingers on sensor to prompt the resident.
- Training capsule provided on the device for operator training, as sequence of images or videos to enable best fingerprint image capture.
- Prompting the resident during fingerprint capture - resident and operator benefit from prompting signals implemented on device/sensor and helps in achieving high quality fingerprint captures.
    - Prompting can be achieved with a sound to signal starting time of capture
    - In case, option to light up sensors exists or providing lights around the sensor is possible, same can be considered.
    - Signaling end of capture to operator is important and helps during multiple captures.
- Authentication should not attempt to alter either minutiae or image record.

6.3.8 IRIS Authentication Application

Authentication focuses on matching a person's identity based on the reliability of a credential offered. Various agencies have different requirements for the degree of assurance required while authenticating residents.

When using IRIS, at a high level, there are three distinct activities:

1. Authentication device capture the IRIS image and send to the UIDAI server along with AADHAAR number for authentication.
2. The IRIS image and AADHAAR number is matched with the available templates, provided at the time of enrollment, in the Data Center.
3. The Data center reply with a Yes or No for every match. If the response is yes then it states that the resident is authenticated and vice-versa.

IRIS based authentication is supported through "kind 7" image formats compliant to ISO 19794-6 standard [ISO 19794-6, 2011].

IRIS Authentication Process:

1. AUA devices using biometric authentication implementing authentication API can benefit from the best known methods.
2. The operator enters the AADHAAR no into the application and captures IRIS image of the resident through the IRIS Capture device.
3. Prompting the resident during IRIS capture - resident and operator benefit from prompting signals implemented on device/sensor and helps in achieving high quality IRIS captures.
    - Prompting can be achieved with a sound to signal starting time of capture
    - In case, option to light up sensors exists or providing lights around the sensor is possible, same can be considered.
4. Signaling end of capture to operator is important and helps during multiple captures
5. The packet containing the IRIS and AADHAAR no. is sent to the CIDR through ASA network for authenticating the resident.
6. The packet data is extracted at CIDR and the AADHAAR no. and the IRIS image is matched with the available templates in the data center, capture at the time of enrollment of the resident.
7. The CIDR response to the operator in just yes or no.
8. If the set of match is successfully found in the CIDR data then it returns 'Yes' to the operator and the resident is successfully authenticated.
9. If the set of data is not successfully matched then it returns with a 'No' and it means the resident is not authenticated successfully and the operator need to authenticate again following the same procedure or need to user other modalities as fingerprint, OTP or demographic details for Authentication.

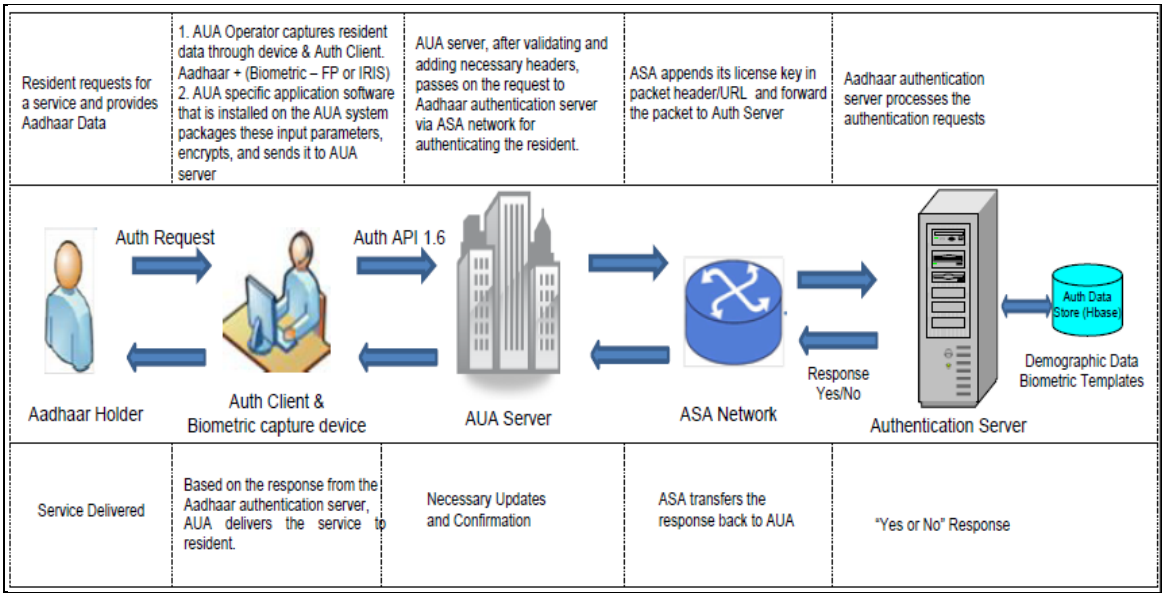


Figure 10: Authentication Process Flow

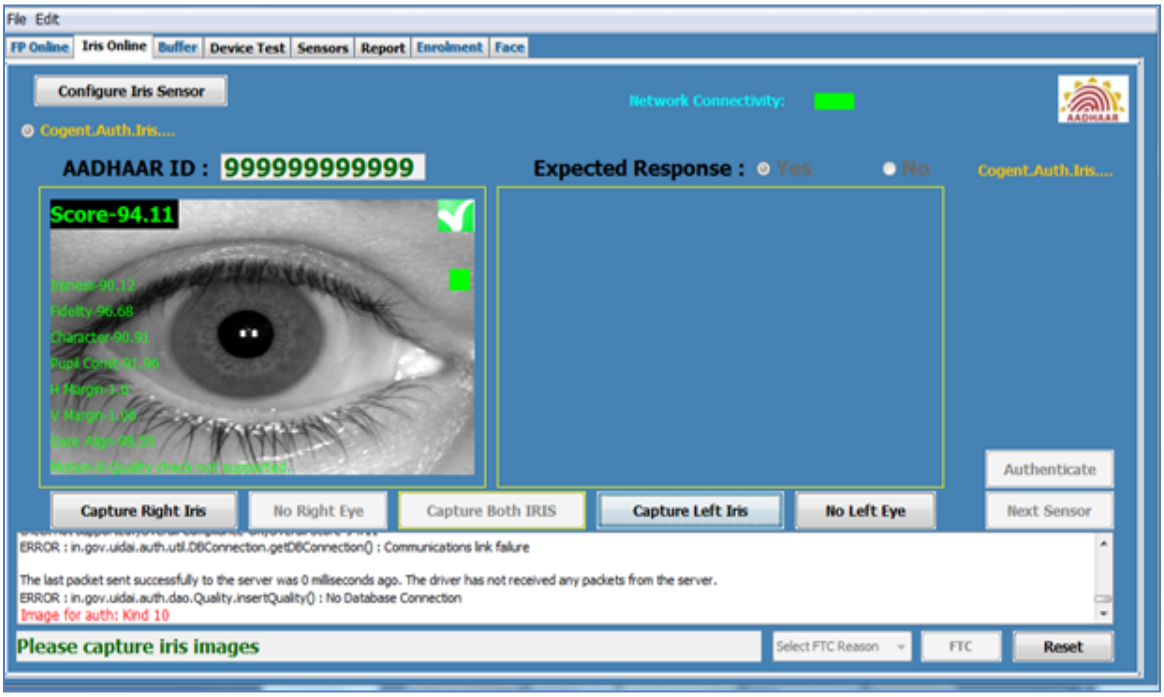


Figure 11: IRIS Capture Image

6.3.8.1.1 OTP Authentication Application

Authentication focuses on matching a person's identity based on the reliability of a credential offered. Various agencies have different requirements for the degree of assurance required while authenticating residents.

When using OTP, at a high level, there are two distinct activities:

1. Application requesting OTP to be sent to resident's mobile. After the successful API invocation, a newly generated random OTP is sent to resident's mobile.

2. Application using the OTP value sends it to UIDAI server for authentication through AUA-ASA network.

Since OTP usage assumes that the resident is present during the transaction (to be able to provide the OTP value received on his/her mobile for subsequent authentication transaction), only a maximum of one OTP is valid for an Aadhaar number at any point in time. Every time a new OTP is generated, previous OTP cease to be valid. OTP generated has an expiry period for security reasons and it is expected that resident uses the OTP within a reasonable time. If not used, OTP expires and a new OTP needs to be generated for next transaction.

OTP Request Process

The OTP request work flow is listed below:

1. An Application, wants to use Aadhaar OTP as a factor within Aadhaar Authentication initiates the transaction flow.
2. Application captures Aadhaar number along with other attributes (name, address, biometric, etc.) as needed by the application
3. Application, through AUA-ASA server, sends the OTP request to UIDAI server.
4. The UIDAI server processes the input, validates it, generates OTP, and sends it to resident's registered mobile and email (based on Aadhaar data in UIDAI server)
5. The Residents receives the OTP on his/her mobile and/or email.
6. The Application then requests the resident to enter the OTP into the application so that application can send it for Aadhaar Authentication.

If OTP has not expired and it matches with the other authentication factors then application responds with a "**Yes** / **No**" with a return code.

Note: OTP expires with a UIDAI stipulated time. OTP message sent to resident provides time at which OTP was generated and the duration when it is going to expire. Since OTP is always sent to both mobile and email of the resident, resident can use the OTP received in his/her mobile/email while authentication.

Sample Applications UIDAI has developed sample vanilla authentication applications which could be consumed by AUAs to integrate with their Aadhaar Applications. Details of the applications are available at **https://developer.uidai.gov.in/site/downloads**

UIDAI has published API's which need to be used by Authentication User Agencies (AUA's) in their application if using Aadhaar biometric authentication.

The API details are available in the URLs mentioned below:

Sr. No.	Application	URL Details
1	Aadhaar Authentication	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf
2	Aadhaar One Time PIN (OTP)	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf
3	Aadhaar Best Finger Detection (BFD)	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf

Authentication Error Handling

It is really important to handle Authentication API errors correctly. Authentication Application should have provisions to handle these errors. Details guidelines to handle exception in application are mentioned at below URL: https://developer.uidai.gov.in/site/node/39.

Standards and Specifications

UIDAI has published Security Policy Specifications and Standards for AUAs and Authentication Devices being deployed by AUAs. Some of the mandatory security requirements which every Authentication application should adhere to are:

- PID block captured for Aadhaar authentication should be encrypted during capture and should never be sent in the clear over a network.
- The encrypted PID block should not be stored unless it is for buffered authentication for a UIDAI specified period of time.
- Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database.
- In the case of operator assisted devices, operators should be authenticated using mechanisms such as password, Aadhaar authentication, etc.
- In case of the OTP Authentication it is mandatory to have beneficiary residents at the point of authentication initiated.

For further details on UIDAI Authentication Standards and Specifications please refer
http://uidai.gov.in/images/authentication_standards_and_specs_v1_7.pdf

6.4 Compliance

6.4.1 Audit

AUAs have to ensure that its operations and systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body before commencement of its operations and it has to provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, as specified by UIDAI.

UIDAI recommends following guidelines (which may be revised at the sole discretion of UIDAI) for audit to be undertaken by an ASA/AUA.

List of Documents to be referred for the Audit Purposes

The documents mentioned below details the standards, policies and specifications for AUAs to follow to ensure secure, reliable and continuous Aadhaar authentication services.

S. No	Document	Description
1.	Aadhaar Authentication Standards and Specifications	This document provides list of various standards and specifications for compliance by an AUA and the link/reference to the respective document/resource
2.	UIDAI-AUA Agreement	Various obligations of the AUA as detailed in the UIDAI-AUA agreement signed with UIDAI

Audit report submission
Audit report/ certificate duly signed by auditor and certified by AUA should be submitted to the UIDAI as per schedule below:

a. AUA should submit the report/ certificate to UIDAI prior to the commencement of operations

b. AUA should submit annual compliance report, upon request by UIDAI, within 30 days of such request by UIDAI

6.4.2 Testing

AUAs thus have to ensure that its operations and systems work seamlessly with the various components of the entire delivery systems. Any disruption in the end to end delivery chain may result in denial of service. Thus it is important for the AUAs to test the entire process and the delivery chain end to end, with all the possible permutations and combinations.

So an AUA is required to complete end to end testing for ensuring the developed AUA server and device applications connects with ASA application and through ASA to UIDAI database (CIDR). The testing should be carried in three stages as listed below:

1. Testing on UIDAI development testing environment: AUA tests the authentication application by transmitting authentication transactions to UIDAI development environment. For details on the development environment testing please refer UIDAI Developer at https://developer.uidai.gov.in/site/.

2. Testing for ASA connectivity on ASA testing environment: AUA is expected to complete the testing with ASA server applications on development environment. AUA is expected to engage an UIDAI approved ASA in earlier stages to develop the link between AUA and ASA server which will be used in this stage to perform integration testing for successfully transmitting the authentication requests. In certain scenarios, depending on the ASA architecture and testing environments an AUA could achieve this only after obtaining the AUA pre-production code from UIDAI.
3. Testing for end to end connectivity on UIDAI pre-production environment: AUA need to request for AUA code and license key by sending an email to UIDAI authentication support team at authsupport@uidai.gov.in. Once the details are received, AUA would need to get in touch with engaged ASA to transmit the transactions to UIDAI pre-production environment. Please note that the request from AUA for accessing the pre-production environment will need to go through an internal approval process of UIDAI where the team ensures that the AUA has signed the UIDAI-AUA agreement and the AUA has entered into an agreement with an UIDAI approved ASA.

Key areas for testing that an AUA may consider for end to end implementation and testing are:

The integration of domain application with Aadhaar authentication
Aadhaar authentication process is just a facilitator for the AUAs and provides authentication services for their domain process. It is important that AUA architect the system in way that both the domain process and Aadhaar authentication process co-exists and support each other.

Example: A successful Aadhaar Authentication should facilitate domain process for service delivery and a failed authentication process should lead to exception handling in the domain process.

The transaction between various touch point and process hubs

A typical AUA process involves transaction initiated from a device (like MicroATM), going to an AUA server, then to an ASA server (for Authentication), then to CIDR and back.

There are various challenges at each of this transaction points and process hubs.
Like transaction between the device and the AUA server will contain both Aadhaar authentication info and domain specific information. However the connectivity between these two points may have very limited bandwidth. Hence there is a challenge to keep the packet size low and ensure that it works on lower possible bandwidth.

Further the transaction between the AUA and ASA is based on certain requirements like the packet to be signed.

6.5 Roll out

6.5.1 Go Live and Training

6.5.1.1 *Go Live*

At this stage an AUA ensures that all the previous stages and their activities are completed to proceed with the Go Live checklist for getting access to UIDAI production environment. By this stage an AUA would have sent confirmation for compliance to the current standards and specifications as published by UIDAI to get production AUA code and license key for creation of the authentication requests.

Sr No	Activities	AUA
1	AUA has arranged for infrastructure for digital signature and tested in Pre-production environment	☐
2	The Public key corresponding to Digital signature infrastructure submitted to UIDAI	☐
3	The format of public key is X.509	☐
4	AUA has conducted end-to-end testing for 100 no of successful transactions in Pre-production environment	☐
5	AUA data logging for Authentication Audit trail being provisioned	☐
6	AUA is ready to deploy devices with STQC certified sensor-extractor, if using biometric authentication and FDC code(s) have been arranged (Refer Aadhaar Authentication API Document, pg 14 & 15)	☐
7	UDC Nomenclature Defined	☐
8	Domain Application is ready for deployment	☐
9	Client Application has provisioned for BFD, two Finger Authentication, UDC, Location configuration and Operator login in case of operator assisted devices. (Refer Aadhaar Authentication & BFD API)	☐
10	Obtained certificate from an information systems auditor certified by a recognized body for compliance to UIDAIs standards and specifications	☐
11	Resident consent process to obtain consent is ready to be deployed	☐

6.5.1.2 *Operator Training*

AUAs are required to deliver training modules developed for operators who would be interacting with residents for service delivery. The training delivery should focus on the following areas:

- Usage of biometric devices and Do's / Don'ts for capturing good quality biometrics.
- Usage of BFD, process for on-boarding residents and guiding residents for next steps.
- Exception handling processes (as adopted by the AUA) and ensuring no denial of service to residents due to technology limitations.
- Communicating appropriately with residents.
- Fraud monitoring and fraud reporting guidelines.
- Basic troubleshooting steps and contact details of AUA's device/application support team.
- Client application (as per the software deployed by the AUA).
- Process steps (of the AUA) for handling resident requests.
- Point of Sales /device operations and handling.
- To avoid duplicate requests.

UIDAI has developed standard training modules that could be integrated with AUAs business and applications training modules. For details of the training modules please refer UIDAI website www.uidai.gov.in/auth or contact UIDAI support team.

6.5.2 Release and Operate

6.5.2.1 *Indicative Deployment View*

Initially AUA can start with providing services using restful web service. These services can be accessed using http or https protocol. Figure below depicts possible indicative deployment architecture (assuming clustered environment) for such setup. This does not cover in detail communication setup between AUA and ASA as it will vary for every AUA and ASA. So link from Application server to ASA is to just for completing the view in real setup there may be different component in between AUA application server and ASA.

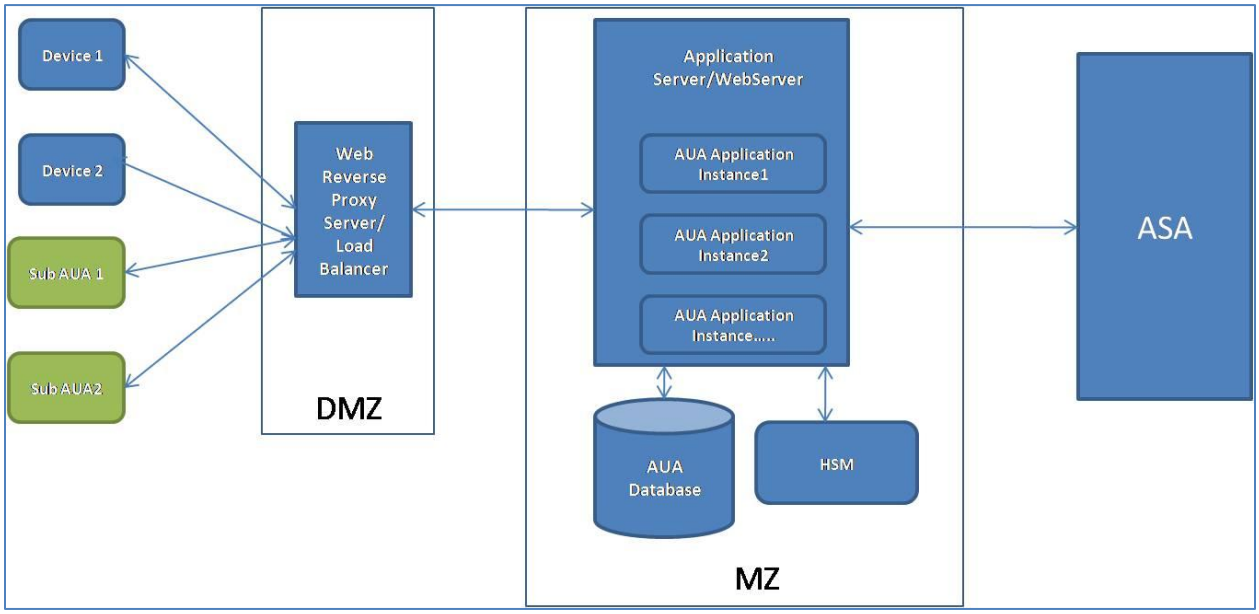


Figure 12: Indicative Deployment Architecture

Devices/Sub AUAs can access AUA rest web services through http/https protocol. Request can hit on a proxy server/load balancer which in turn can forward that request to appropriate instance of AUA application and further AUA application can call ASA application and similarly response can be transferred back to end device/Sub AUA.

7 Suggestions to Improve Authentication Success Rate

A high success rate is the hallmark of a successful online authentication process. To this day, about 2 Crore authentication transactions have been carried out with a success rate of over 92%. Out of the 8% rejects, a major chunk is actually true rejects. It is practically seen that if there are no seeding problems or fraud attempts the success rate is close to 98% in case of fingerprint and potentially higher with iris. It has also been observed during various pilot efforts underway that rejects can be substantially brought down by following laid down procedure and in cases where authentication failure persists, performing the diagnostic procedures specified by UIDAI (Best finger detection for example for fingerprint authentication) helps in resolving the issues. Rejects can be handled most times through laid-down procedures than needing any technical solution.

Rejects can be further classified into two - True rejects and False rejects.

7.1 Reasons of True rejects and ways to avoid the same

A true reject should not be permitted to repeat. The success of the system will largely depend on discerning true rejects and prevention of a repeat of rejection of the same Aadhaar number.

#	Reasons	Solutions.
1	Seeding problem	There should be daily Feedback mechanism where the users (AUA) should be intimated clearly of the rejected UID numbers, to help investigate and eliminate seeding errors. **Implementation of Verhoeff algorithm in application will largely prevent any clerical error in seeding.**
2	Fraud Attempts – Cases where multiple attempts are made to authenticate against a particular UID.	Rules and guidelines to prevent Fraud Authentication attempts should be promulgated as deterrence.

7.2 Recommendations

1. Device:

- Usage of certified devices is important.
- Device Nomenclature needs to be implemented.
- Device Registration process will improve device traceability.
- Provision to track the location of the device, through Pincode, Geo Tagging etc. is also helpful
- Provision to track the extractor version of the device needs to be explored

2. Client Application:

- **C**ompliance of the client application as per the backend infrastructure & guidelines issued by UIDAI.
- **Following Standard operating process for fingerprint Authentication**
    - Application should mandatorily take the resident's 2 fingers (fusion) at least three times before getting into exception handling tracks (offline/manual validation of the genuineness of the resident)
    - Application should have a feature to mandatorily accept quality capture only. I.e. if the quality of the capture is bad, application should prompt the resident to try again, do BFD etc.
    - If a compliant finger print authentication (BFD+ Multi finger + Multiple try) fails the application should prompt the resident for trying other authentication factors, wherever feasible (OTP for example)
- **Following Standard operating process for IRIS Authentication**
    - Applications implementing IRIS authentication should follow the process outlined in the IRIS authentication proof of concept report. It is recommended that three presentations and three attempts till authentication success is achieved is mandatorily implanted in the application.
    - **Single eye camera**: Each presentation is defined as image of one eye. Second attempt used different eye from the first. In other words, the recommended multiple attempt sequence is right eye, left eye, right eye and so on. The switching of eyes effectively provides "best finger" strategy for two eyes.
    - **Dual eye camera**: Each presentation is defined as one image of each eye (two iris images). Here again, the three attempts should be mandatorily implemented in order to achieve high degree of success. Dual eye camera is effectively equivalent to using two fingers for authentication.
    - Application should have a feature to mandatorily accept quality capture only. I.e. if the quality of the capture is bad, application should prompt the resident to try again.
    - Application should prompt residents to try other authentication factor after repeated failure using iris – examples of other factors include fingerprint, OTP where feasible.

3. Process & Policies:

- Audit process and policies for Authentication Client Application to be in place.
- Guidelines to prevent Fraud Authentication attempts being introduced into the system.
- Device registration policy to be in place.

4. Process Compliance:

- Suggest residents to undergo BFD, perform multi finger authentication, attempt at least 3 times in case of authentication rejects.

5. Authentication Transaction Reporting:

- Log "Server not available" errors separately as Error transactions and not include in the total Authentication Transaction count. This would reduce the inconsistency between the volume projected by AUA's and UIDAI.

6. Operator Training/Material

- Training Manual to be developed for operator trainings.

7. Usage of Poster and Campaigns

- Posters on Authentication or BFD processes need to be made available in and around the service delivery counters/shops.
- Campaigns are required to create awareness among the residents on the benefits of Aadhaar-based service delivery, and the right usage of the applications/devices.

8. **Verhoeff Algorithm**

- An MS Excel utility containing Verhoeff algorithm (available freely, can be provided) could be used with the client application, so that the incorrect UIDs can be captured during seeding. This will reduce error 998 from the field.

7.3 Best Practices

S. No	Dimension	Emerging Best Practices
1.	Device Sensor/Extractor	• Usage of certified Devices/Sensors/ Extractors • Operator training for appropriate usage of devices • Tracking mechanism for devices being used by AUAs • Device should have capability to connect to any type of internet sources – USB, LAN Cable, Telephone cable etc • Devices should have support for external Antenna in case of low connectivity areas.
2.	Client Application Compliance	• Usage of Auth Client applications which are compliant to the backend application. • Best practices like usage of BFD, 2 finger Auth being catered to by the Client Application and Similarly for IRIS authentication, use 3 attempts of 3 presentations. • Client application should facilitate clarity in the 'action items' based on the error codes. • A unique device code (UDC)for the authentication device assigned within the AUA domain {UDC should be an alpha-numeric string of maximum length 20}. This allows better reporting and tracking of the client devices and should be

		mandatorily used during authentication transaction. The same can be used to provide specific feedback regarding the device specific behaviours.
3.	AUA Operators	• Operator Trainings being performed. • Enhance understanding about Error Codes generated by system and corresponding actionable.
4.	Enrolment capture Quality	• Identify errors due to bad biometric capture quality during enrolment process, and suggest reenrolment to the residents
5.	Two Finger Authentication & BFD	• Enforce usage of 2 finger authentication, BFD to improve auth accuracy.
6.	Aadhaar Seeding	• Ensure that the Aadhaar number seeding is done correctly by the AUAs to eliminate seeding errors.

8 Appendix

8.1 Related Publications/ Tools

Sr. No.	Description	URL/ Location	Description
1	Aadhaar Authentication Strategy Document	http://uidai.gov.in/images/authDoc/auth_strategy_creating_a_circle_of_trust.pdf	
2	Aadhaar Authentication Operating Model	http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf	
3	UIDAI-AUA Agreement Template	http://uidai.gov.in/images/FrontPageUpdates/d3_6_uidai_aua_agreement_v2_1.pdf	
4	AUA Application form	http://uidai.gov.in/images/aua_application_form_ver1_4.pdf	
5	List of support documents and application process	http://uidai.gov.in/images/FrontPageUpdates/asa_aua_application_process_v2.pdf	
6	Guidelines for AUA-ASA Agreement	http://uidai.gov.in/images/authDoc/d3_6_guidelines_for_the_agreement_between_asaaua_v1.pdf	
7	Guidelines for AUA-Sub AUA Agreement	http://uidai.gov.in/images/authDoc/d3_6_guidelines_for_the_agreement_between_aua_asa_v1.pdf	
8	Aadhaar Authentication Standards and Specifications	http://uidai.gov.in/images/FrontPageUpdates/authentication_standards_and_specs_v1_7.pdf	
9	Illustrative Template of Resident Consent Form for Aadhaar Authentication	http://uidai.gov.in/images/FrontPageUpdates/resident_consent_form_for_aadhaar_authentication_illustrative_template_v1_0.pdf	
10	UIDAI Empanelled Consultants	http://uidai.gov.in/images/FrontPageUpdates/final_empanelment_list_30_may_2011.pdf	
11	Aadhaar Developer Portal	http://developer.uidai.gov.in/site/	Provides client software, APIs, Authentication Sample application and Technical papers

12	Aadhaar Authentication Discussion Group	https://groups.google.com/forum/#!forum/aadhaarauth	Group to encourage collaboration between development community by facilitating Aadhaar Authentication related technical and integration discussions
13	UIDAI Authentication Application Developer Portal	https://developer.uidai.gov.in/site/auth_basics	
14	Authentication API	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf	
15	Best Finger Detection API	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf	
16	Technology FAQs	http://developer.uidai.gov.in/site/auth_tech_faqs	
17	Demographic Data Standards	http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf	

8.2 Glossary of Terms and abbreviations

Sr. No.	Term/ Abbreviation	Description
1	API	Application Program Interface
2	ASA	Authentication Service Agency
3	AUA	Authentication User Agency
4	BFD	Best Finger Detection
5	CIDR	Central Identities Data Repository
6	STQC	Standardization Testing and Quality Certification
7	UIDAI	Unique Identification Authority of India
8	IRIS	Image Recognition Integrated Systems
9	OTP	One Time Pin

Eligibility Criteria for on-boarding AUA / KUA

Unique Identification Authority of India
Niti Aayog, Govt. of India
Jeevan Bharati Building
Connaught Circus
New Delhi 110001

No. K-11020/45/2012-UIDAI (Auth)

Release Date: 06-Aug-2015

Version 1.0

1. Introduction of Aadhaar:

1. The Unique Identification Authority of India (UIDAI) has been established by the Government of India in January 2009, as an attached office to the Planning Commission, now NITI Aayog. The mandate of the Authority is to issue a unique identification number (called Aadhaar or UID) to Indian residents that is robust enough to eliminate duplicate and fake identities, and can be verified and authenticated using biometrics in an easy and cost-effective manner.
2. In this context, the UIDAI collects the demographic and Biometric data of residents of India. After de-duplication, it issues a Unique Identification Number to the resident, which is a 12 digit random number. UID number is being delivered to the residents in the form of a laminated letter through post. Various Central Government Departments, State Governments and Financial Institutions like Banks and LIC have been partnered as 'Registrars' and are collecting the data with the help of Enrollment Agencies across the country.
3. The UID has been envisioned as a means for residents to easily and effectively establish their identity, to any agency, anywhere in the country, without having to repeatedly produce identity documentation to agencies. More details on the UIDAI and the strategy overview can be found on the website: http://www.uidai.gov.in

2. Aadhaar Authentication Service

Aadhaar Authentication is defined as the process wherein, Aadhaar number along with the Aadhaar holder's personal identity information is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it.

The purpose of Authentication is to enable Aadhaar-holders to prove identity and for service providers to confirm the resident's identity claim in order to supply services and give access to benefits. Aadhaar Authentication shall make life simpler to the resident as it is meant to be a convenient system to prove one's identity without having to provide identity proof documents whenever a resident seeks a service.

UIDAI offers Aadhaar-based authentication as a service that can be availed by government / public and private entities/agencies that wish to authenticate the identity of their customers / employees / other associates (based on the match of personal identity information) before providing them access to their services / business functions / premises, etc.

Some key features of Aadhaar authentication service are:

a) UIDAI is offering Aadhaar-based authentication services free of charge till 31st Dec 2015.

b) The use of Aadhaar-based authentication to enable their services / business functions is optional. Government / public / private entities use it only on a voluntary basis.

c) UIDAI encourages user entities to adopt federated authentication system, i.e., a combination of Aadhaar authentication and their own authentication systems. In case of user entities that already have their own authentication systems in place, Aadhaar authentication is envisaged to act in conjunction with existing authentication systems and strengthen the overall authentication rather than replace existing authentication systems.

d) UIDAI shall provide Aadhaar-based authentication services on a best-effort basis. UIDAI shall endeavor to inform and educate potential users of Aadhaar-based authentication and other key actors in the Aadhaar ecosystem of the benefits, risks and implications of using Aadhaar-based authentication. UIDAI is not liable for results of authentication to the agencies that use Aadhaar-based authentication to enable their services.

e) Aadhaar authentication services cannot be used for purposes that are anti-Government, anti-State, illegal, discriminatory or related to money laundering.

3. Aadhaar e-KYC (Know your customer) Services

UIDAI offers the e-KYC service, which enables a resident having an Aadhaar number to share their demographic information and photograph with a UIDAI partner organization in an online, secure, auditable manner with the residents consent. The consent by the resident can be given via a Biometric authentication or One Time Password (OTP) authentication.

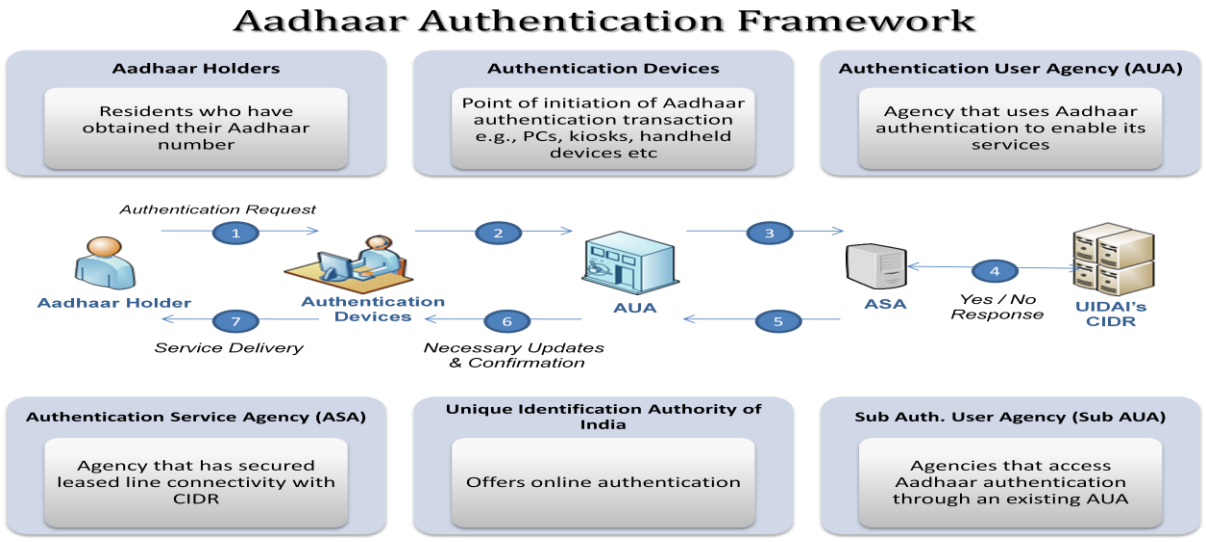
The Aadhaar holders demographic information i.e. Name, Address, Date of Birth, Gender, Phone & Email (where available) & Photograph which is currently available with the resident is shared via the e-KYC service.

Some of the key features of the e-KYC service are:

a) Paperless: The service is fully electronic, enabling elimination of KYC document management
b) Consent based: Data is shared by the resident consent through Aadhaar authentication, thus protecting resident privacy.
c) Secure and compliant with the IT Act: Data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper documents.
d) Non-repudiable: The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital signature by UIDAI when providing the e-KYC data makes the entire transaction non-repudiable by all parties involved.
e) Instantaneous: The service is fully automated, and KYC data is furnished in real-time, without any manual intervention
f) Regulator friendly: The service providers can provide a portal to the Ministry/Regulator for auditing all e-KYC requests.

4. Aadhaar Authentication Framework

Aadhaar-based authentication refers to the sequence of events during which the personal identity information / data of an Aadhaar-holder is matched with their personal identity information / data that is stored in the CIDR. An Aadhaar holder's Personal Identity Data (henceforth referred to as PID) includes his or her demographic details, one-time password (OTP with a limited validity period) sent to the Aadhaar holder's cell phone (stored in the CIDR) and the Aadhaar holder's biometric information (fingerprint and iris scan).



4.1 Authentication User Agency (AUA)

AUAs are agencies that uses Aadhaar authentication to enable its services and connects to the CIDR by an Authentication Service Agency (ASA). AUA may also engage more than one ASA. An AUA could also transmit authentication requests from other entities that are "Sub AUAs" under it (see details on Sub AUA below). AUAs can also act as an aggregator offering authentication services to Sub-AUAs below them and may also offer value added services such as multi-party authentication, MIS reports and authorization to their Sub AUAs. An AUA enters into a formal agreement with UIDAI in order to access Aadhaar authentication.

Number of sub-AUAs authorized to be engaged by each AUA will be based on the number of transactions as mentioned below:

	Average monthly transactions in last 3 months	**Number of sub-AUAs allowed**
Category A	Above 5 Lakh	Unlimited
Category B	2 – 5 Lakh	50
Category C	1 - 2 Lakh	10
Category D	Less than 1 Lakh	0

Note: Entities under category 1, 2.1.1, 2.1.2, 2.1.5, 2.2, 2.3 are exempted from the transaction requirements and may engage unlimited number of sub-AUAs.

4.1.1 Sub AUA

An agency / entity (any legal entity registered in India) desiring to use Aadhaar authentication to enable its services could access Aadhaar authentication services through an existing AUA. The following are some possible examples:

(i) Government of any State/Union Territory could become an AUA and several ministries/departments in the State could access Aadhaar authentication services through the State government as its Sub AUAs.

(ii) A small entity or business (e.g. a small scale bank) which does not want to directly engage in a formal agreement with UIDAI but still wants to use Aadhaar Authentication, may choose to access Aadhaar services as a Sub AUA of an existing AUA (e.g. a large bank or any aggregator AUA offering AUA services).

(iii) Several entities could combine under a single AUA for business reasons. Ex. several hotels could access Aadhaar authentication as Sub AUAs of an Hoteliers Association that becomes an AUA.

In all such cases UIDAI has no direct contractual relationship with the Sub AUA. Only the AUA is contracted to UIDAI and shall be responsible for all authentication requests flowing through it, including those originating from its Sub AUAs. Upon appointment of sub-AUA, an AUA need to share the copy of the agreement between AUA and sub-AUA with UIDAI. AUA is liable to share the details of sub-AUA such as sub-AUA Organization details, Business scope, code etc.

4.2 Authentication Service Agency (ASA)

ASAs are agencies that have established secured leased line connectivity with the CIDR 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 agencies 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 reports to AUAs. An ASA is bound to UIDAI through a formal agreement.

4.3 e-KYC User Agency (KUA)

e-KYC User Agency (KUA) means Authentication User Agency that is eligible for the e-KYC service. KUA uses Aadhaar e-KYC to enable its services and connect to the CIDR through an e-KYC Service Agency (KSA). e-KYC means the transfer of demographic data (such as Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph collected by UIDAI in the form of a digitally signed XML document to an Authentication User Agency, through an Authentication Service Agency, based on resident authorization received by UIDAI in the form of successful biometric or OTP-based Aadhaar authentication. KUA enters into a formal agreement with UIDAI in order to access Aadhaar authentication e-KYC services. KUAs can also act as an aggregator offering authentication services to sub-AUAs

below them and may also offer value added services to their Sub AUAs. However, KUAs are not authorized to offer e-KYC services to their sub-AUAs.

4.4 e-KYC Service Agency (KSA)

e-KYC Service Agency (KSA) means Authentication Service Agency that is eligible to provide access to the e-KYC service through their network. KSAs are agencies that have established secured leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. KSAs offer their UIDAI-compliant network connectivity as a service to e-KYC User Agencies and transmit KUAs' authentication requests to CIDR and in return share the response in the encrypted format from CIDR to e-KYC User Agencies.

5. Aadhaar Authentication system supports the following Authentication modalities:

1. Biometric Matching
    a. Finger Print Authentication
    b. IRIS Authentication
2. Demographic Matching
3. One-Time-PIN (OTP)

5.1 Biometric Matching

Biometric Matching refers to the usage of Aadhaar Authentication for matching the biometric data (Finger Prints or IRIS) submitted by the resident (captured through an authentication device) with the biometric attributes of a resident stored in the UIDAI database (CIDR) and return the response in Yes (Successful Authentication) or No (Failed Authentication).

5.2 Demographic Matching

Demographic matching refers to the usage of Aadhaar Authentication system for matching the Aadhaar number and demographic data of the resident in the AUA/Service provider database or with demographic data obtained at the point of authentication with the demographic attributes (name, address, date of birth, gender, etc. as per API specifications) of a resident in the UIDAI database (CIDR) and return the response in Yes (Successful Authentication) or No (Failed Authentication).

5.3 One-Time-Pin

In case of matching using One-Time-PIN (OTP) an OTP is sent to the registered mobile number of the resident seeking Aadhaar Authentication. The OTP shall have a limited validity of 15 min. The resident shall provide this OTP during authentication and the same shall be matched with the OTP sent by the UIDAI and returns the response in Yes (Successful Authentication) or No (Failed Authentication).

6. Aadhaar e-KYC system supports the following Authentication modalities:

1. Biometric Matching
    a. Finger Print Authentication
    b. IRIS Authentication
2. One-Time-PIN (OTP)

6.1 Biometric Matching

Biometric Matching refers to the usage of Aadhaar Authentication for matching the biometric data submitted by the resident (captured through an authentication device) with the biometric attributes (Finger Prints or IRIS) of a resident stored in the UIDAI database (CIDR) and return the response in the form of demographic data (such as Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph in case of successful Authentication or error code in case of failed Authentication.

6.2 One-Time-Pin

In case of matching using One-Time-PIN (OTP) an OTP is sent to the registered mobile number of the resident seeking Aadhaar Authentication. The OTP shall have a limited validity of 15 min. The resident shall provide this OTP during authentication and the same shall be matched with the OTP sent by the UIDAI and returns the response as demographic data (such as Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph in case of successful Authentication or error code in case of failed Authentication.

7. Organizational Pre-Qualification criteria to enter the Aadhaar Authentication ecosystem as AUA/KUA

S.No.	Pre-Qualification Criteria	Supporting Documents
1	**Government Organization**	
1.1	A Central/ State Government Ministry/Department and their attached or sub-ordinate offices	1. Letter of Intent by Head of the Department/office expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full)
1.2	An undertaking owned and managed by Central / State Government (PSU)	1. Letter of Intent by Managing Director/Chief Managing Director of PSUs expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the

S.No.	Pre-Qualification Criteria	Supporting Documents
		attested specimen signatures (both initials and full) 3. Letter of establishment of PSU
1.3	An Authority constituted under the Central / State Act/Special Purpose Organization constituted by Central/State govt.	1. Letter of Intent by Head of the Organization/CMD/Managing Director expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Letter of establishment of the Authority
2	**Regulated Service Providers**	
2.1	Regulated / Licensed by RBI – Banks and Payment & Settlement System (Excluding Banks in **Category 3.1.4**)	
	2.1.1 Public Sector Banks (PSB)	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with attested specimen signatures (both initials and full) 3. Valid License issued by RBI and Gazette notification
	2.1.2 Private Banks, Foreign Banks Licensed by RBI to operate in India	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by RBI 4. Certificate of Incorporation 5. Board Resolution for making AUA / KUA application
	2.1.3 Regional Rural Banks	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf

S.No.	Pre-Qualification Criteria	Supporting Documents
		of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by RBI and Gazette notification 4. Certificate of Incorporation 5. Letter of association from PSB
	2.1.4 Co-operative Banks 1. State Co-operative Banks 2. District Co-operative Banks 3. Scheduled Urban Cop-operatives Banks	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by RBI 4. Letter of association from the Centre /State government. 5. Certificate of Incorporation
	2.1.5 Payment & Settlement System Network 1. Financial market infrastructure 2. Retails payments organization 3. Cards payment network 4. ATM networks 5. Pre-paid payment instruments 6. White label ATM operators 7. Instant Money Transfer	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Certificate of Authorization issued by RBI 4. Certificate of Incorporation 5. Board Resolution for making AUA / KUA application
2.2	Regulated by IRDA/ PFRDA - Financial Institutions	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by the regulator (IRDA / PFRDA) 4. Certificate of Incorporation 5. PAN / Service Tax Number / TIN (if any) 6. Board Resolution for making AUA / KUA application

S.No.	Pre-Qualification Criteria	Supporting Documents
2.3	Regulated by TRAI – Telecom	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by DoT for each circle 4. Certificate of Incorporation 5. Board Resolution for making AUA / KUA application
3	**Other Entities**	
3.1	3.1.1 Company registered in India under the Companies Act 1956 / The companies Act 2013 (Company under group of companies has to apply individually)	1. Letter of Intent by CMD/MD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Extract of AOA and MOA mentioning area of operation pertaining to AUA/KUA. 4. Certificate of incorporation 5. Copy of Service Tax Number / TIN / PAN 6. Board Resolution for making AUA / KUA application 7. Certified copy of letter of commencement of business issued by Ministry of Corporate Affairs (MCA)
	3.1.2 Partnership registered under the India Partnership Act 1932 or under the Limited Liability Partnership Act, 2008	1. Letter of Intent by the partners expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Registered Partnership deed. 4. Registration Certificate from Registrar of Firms OR Ministry of Corporate

S.No.	Pre-Qualification Criteria	Supporting Documents
		Affairs (MCA), as applicable 5. Certificate of incorporation 6. Copy of Service Tax Number / TIN / PAN
	3.1.3 Proprietorship firm	1. Letter of Intent by the proprietor expressing interest to onboard as AUA/KUA 2. Letter of Authorization from proprietor to depute Authorized person for the purpose of AUA/KUA 3. Copy of Service Tax Number / TIN / PAN 4. Valid Business Licenses 5. Legal document issued by the state/Local government authority
	3.1.4 Regulated / Licensed by RBI 1. Non Banking Financial Company 2. Non Scheduled Urban Co-operative Banks	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by RBI 4. Certificate of incorporation 5. Copy of Service Tax Number / TIN / PAN 6. Legal document issued by the central/state/Local government authority 7. Certified copy of letter of commencement of business issued by Ministry of Corporate Affairs (MCA)
	3.1.5 Regulated by SEBI - Brokerage firms	1. Letter of Intent by Head of the Department/office expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Valid License issued by SEBI 4. Copy of Service Tax Number / TIN / PAN 5. Extract of AOA and MOA mentioning area of operation pertaining to

S.No.	Pre-Qualification Criteria	Supporting Documents
		AUA/KUA 6. Certificate of incorporation 7. Legal document issued by the central/state/Local government authority 8. Certified copy of letter of commencement of business issued by Ministry of Corporate Affairs (MCA)
	3.1.6 Not-for-profit Organizations (under section 25 under The Companies Act 1956)	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Extract of the Constitution mentioning area of operation. 4. Letter of Authorization from Ministry of Corporate Affairs (MCA)/Central Government 5. Copy of Service Tax Number / TIN / PAN 6. Legal document issued by the central/state/Local government authority. 7. Certificate of incorporation 8. Board Resolution for making AUA / KUA application
	3.1.7 Academic Institutions / Research and Development Organizations	1. Letter of Intent by Head of the Department/CMD/Registrar expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Copy of Service Tax Number / TIN / PAN 4. Letter from concerned regulatory authority such as UGC, AICTE, MCI, DCI, Education Board, Bar council of India etc 5. Certificate of incorporation 6. Board Resolution for making AUA / KUA application

S.No.	Pre-Qualification Criteria	Supporting Documents
		7. Legal document issued by the central/state/Local government authority
	3.1.8 Societies registered under Indian Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The companies Act, 2013 (Sec 8) / Co-operative Society Act 1912	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Constitution Document 4. Copy of Service Tax Number / TIN / PAN 5. Letter of Authorization from Committee 6. Certified copy of the latest Trust Deed or Society's memorandum of Association or Companies 7. Registration Certificate from Registrar of Societies OR Ministry of Corporate Affairs (MCA), as applicable 8. Certificate of incorporation 9. Board Resolution for making AUA / KUA application
	3.1.9 Any other entity which is other than above mentioned categories	1. Letter of Intent by Head of the Department/CMD expressing interest to onboard as AUA/KUA 2. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 3. Extract of AOA and MOA mentioning area of operation pertaining to AUA/KUA 4. Certificate of incorporation 5. Letter of commencement of the Business issued by Ministry of Corporate Affairs (MCA) 6. Copy of Service Tax Number / TIN / PAN (if any) Legal document issued by the central/state/Local government authority

8. Financial Qualification Criteria

S.No.	Pre-Qualification Criteria	Supporting Documents
1	**Government Organization**	
1.1	A Central/ State Government Ministry	Not Applicable
1.2	Department or an undertaking owned and managed by Central / State Government / PSU	Not Applicable
1.3	An Authority constituted under the Central / State Act/Special Purpose Organization constituted by Central/State govt	Not Applicable
2	**Regulated Service Providers**	
2.1	Regulated / Licensed by RBI – Banks and Payment & Settlement System (Excluding Banks in **Category 3.1.4**) 2.1.1 Public Sector Banks 2.1.2 Private Banks, Foreign Banks Licensed by RBI to operate in India 2.1.3 Regional Rural Banks 2.1.4 Co-operative Banks 1. State Co-operative Banks 2. District Co-operative Banks 3. Scheduled Urban Cop-operatives Banks 2.1.5 Payment & Settlement System Network 1. Financial market infrastructure 2. Retails payments organization 3. Cards payment network 4. ATM networks 5. Pre-paid payment instruments 6. White label ATM operators 7. Instant Money Transfer	Not Applicable
2.2	Regulated by IRDA/PFRDA - Financial Institutions	Not Applicable

S.No.	Pre-Qualification Criteria	Supporting Documents
2.3	Regulated by TRAI – Telecom	Not Applicable
3	**Other Entities**	
3.1	3.1.1 Company registered in India under the Companies Act 1956 / The Companies Act 2013 (Company under group of companies has to apply individually) 3.1.2 Partnership registered under the India Partnership Act 1932 or under the Limited Liability Partnership Act, 2008 3.1.3 Proprietorship Firm 3.1.4 Regulated / Licensed by RBI 1. Non Banking Financial Company 2. Non Scheduled Urban Co-operative Banks 3.1.5 Regulated by SEBI - Brokerage firms 3.1.6 Not-for-profit Organizations (under section 25 under The Companies Act 1956) 3.1.7 Academic Institutions / Research and Development Organizations 3.1.8 Societies registered under Indian Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The companies Act, 2013 (Sec 8) / Co-operative Society Act 1912 3.1.9 Any other entity which is other than above mentioned categories **Criteria **** 1. Private/Public Limited companies need to have minimum Rupees 2 (Two) crore of Paid up capital. Above entities other than Private / Public Limited companies need to have Annual turnover of minimum Rupees 5 (Five) Crore during the last Financial year, and	i) Document mentioning authorized and paid up capital. ii) Audited/ Certified financial statements & annual report – Balance Sheet, PL statement of the last financial year iii) Copy of the IT returns for the previous 1 years duly

S.No.	Pre-Qualification Criteria	Supporting Documents
	2. Entity should be in business for minimum of 3 years from date of commencement of Business, and	acknowledged by Income-Tax department
	3. Large Customer base and Aadhaar usage plan to perform minimum 1 Lakh authentication transactions / month after 3 months of getting AUA Production access.	iv) Declaration from the authorized signatory

9. Technical Eligibility Criteria - This criteria is applicable for all the categories

S.No.	Pre-Qualification Criteria	Supporting Documents
1	Backend infrastructure, such as servers, databases etc., required specifically for the purpose of Aadhaar authentication shall be based in the territory of India, and	Declaration from the authorized signatory
2	IT Infrastructure owned or outsourced to carry out minimum of 1 Lakh Authentication transaction per month, and	• Declaration from the authorized signatory • Submit IT Infrastructure details i.e. Server Details, Network Connectivity, Firewall Server, storage capacity, Disaster recovery plan etc.
3	Data Privacy policy to protect beneficiary privacy, and	Share the data privacy policy on organization's website
4	Data security measures as per the IT Act, and	Certification / Declaration from the authorized signatory

**** Exception to meet the above mentioned financial and technical criteria for Category 3:**

1. **Sub-AUA** who has performed minimum 10,000 transactions / month for last 10 months or minimum 25,000 transactions / month for last 4 months is eligible to become an AUA. The sub- AUA is responsible to submit proof of having performed the desired number of authentication transactions using his sub-AUA code.
2. **Startup** who is among the top 3 awardees in Aadhaar based Hackathon organized with minimum 100 participants would be eligible for provisional AUA with relaxation on technical and financial eligibility criteria. The startup need to perform minimum 1 Lakh authentication transactions in a maximum period of 18 months after getting AUA production access to become regular AUA.

Note: Test data to be excluded from the number of transactions. Live transaction data in Production environment using any modality for Authentication is counted for the purpose.

10. Additional eligibility criteria for KUAs falling under Category 3

Option A (AUA to KUA): Fast Track

1. Private/Public Limited organizations need to have minimum Rupees 4 (Four) crore of Paid up capital. Other organizations under category 3.1 need to have Annual turnover of minimum Rupees 10 (Ten) Crore during the last financial year, and
2. Perform minimum 3 Lakh transactions in a maximum period of 3 months in AUA Production environment till date of Application for KUA

Option B (AUA to KUA): Regular Track

1. Private/Public Limited organizations need to have minimum Rupees 2 (Two) crore of Paid up capital. Other organizations under category 3.1 need to have Annual turnover of minimum Rupees 5 (Five) Crore during the last Financial year, and
2. Minimum 3 months as AUA in Production environment, and
3. Performed minimum of 1 Lakh transactions / month in AUA Production environment in the last 3 months

11. Information for applying as AUA/KUA

Application Fee (Category 3 Other Entities)	Non-refundable Application Fees of Rupees 5,000 /- (Five thousand only) in the form of Demand Draft drawn in favor of "PAO, UIDAI, New Delhi" payable at New Delhi.
Agreement signing Window	An entity needs to sign the agreement within 45 days after the application approved by UIDAI.
Tenure of Agreement	The agreement shall be in force for 5 years (five years) subject to adherence to the terms and conditions of the agreement. No changes with respect to agreement terms will be admissible.
Extension of Agreement	The agreement may be extended based on the requirement and approval by UIDAI
Termination of Agreement	Notwithstanding the duration of the agreement the termination of the agreement is subject to the conditions as mentioned in Clause 10 of AUA / KUA Agreement
Right to Accept / Hold / Seek more information	UIDAI reserves the right to 1. Accept or hold any AUA entities applications 2. Hold the process and applications at any time without thereby incurring any liability to the affected applicant(s) or any obligation to inform the affected applicant(s) of the grounds for such decision.

Dis-qualification	UIDAI may at its sole discretion and at any time during the evaluation of application, disqualify any applicant, if the applicant: (i) Made misleading or false representations in the forms, statements and attachments submitted as proof of the eligibility requirements; (ii) Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years; (iii) Was declared ineligible/blacklisted by the Government of India/State/UT Government;
Service Level Expectations	**From AUA** 1. Shall sign the agreement within 45 days from application approval. 2. Shall migrate from pre-production to production environment in 90 days and further extension of 60 days 3. Perform average of 50,000 transactions / month (after 2 months of being in Live environment) **From KUA** 1. Shall sign the agreement within 45 days from application approval. 2. Shall migrate from pre-production to production environment in 90 days and further extension of 60 days 3. Perform average of 80,000 transactions / month (after 2 months of being in Live environment) • The performance of AUA and KUA would be reviewed and evaluated on Annual basis and failure to meet the above mentioned Service Level Expectations could result in warning followed by suspension of service if no action is taken. • UIDAI reserves the right to audit the AUA, sub AUA and KUA and seek reports on performance, security and data privacy and also undertake audit may be considered necessary

Note: Any relaxation in the Financial, Technical and other criteria mentioned in this document can be considered for relaxation by the competent authority on case to case basis.

12. Organization details to be shared for applying as AUA/KUA

S.No.	Organization Details	To be updated by an entity
1	Name of the Entity	
2	Registered Address	
3	Organization Type	

4	Industry Sector	
5	Year of establishment and constitution of firm/company	
6	Certification from any regulatory body	
7	Name and designation of the person authorized to make commitments to UIDAI *(Certificate of Authority to be provided)*	
8	Telephone and Fax Number	
9	E-mail address	

13. Documentation to be submitted for on-boarding as AUA/KUA

S.No.	Pre-Qualification Criteria	On-Boarding Documents
1	**Government Organization**	
1.1	A Central/ State Government Ministry/Department and their attached or sub-ordinate offices	1. Application should be signed by authorized signatory along with the official seal of the organization 2. Letter of Intent by Head of the Department/office expressing interest to onboard as AUA/KUA 3. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 4. Letter of association from ASA 5. Scope Document 6. 2 copies of blank Stamp Papers of requisite denomination as per the state 7. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria
1.2	An undertaking owned and managed by Central / State Government / PSU	1. Application should be signed by authorized signatory along with the official seal of the organization 2. Letter of Intent by Managing Director/Chief Managing Director/Head of PSUs expressing interest to onboard as AUA/KUA 3. Letter of establishment of PSU 4. Letter of authority, authorizing the signatory to sign documents on behalf of the organization

S.No.	Pre-Qualification Criteria	On-Boarding Documents
		along with the attested specimen signatures (both initials and full) 5. Letter of association from ASA 6. Scope Document 7. 2 copies of blank Stamp Papers of requisite denomination as per the state 8. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria
1.3	An Authority constituted under the Central / State Act/Special Purpose Organization constituted by Central/State govt.	1. Application should be signed by authorized signatory along with the official seal of the organization 2. Letter of Intent by Head of the Organization/Managing Director expressing interest to onboard as AUA/KUA 3. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 4. Letter of association from ASA 5. Scope Document 6. 2 copies of blank Stamp Papers of requisite denomination as per the state 7. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria
2	**Regulated Service Providers**	
2.1	Regulated / Licensed by RBI – Banks and Payment & Settlement System (Excluding Banks in **Category 3.1.4**)	
	2.1.1 Public Sector Banks (PSB) 2.1.2 Private Banks, Foreign Banks Licensed by RBI to operate in India 2.1.3 Regional Rural Banks 2.1.4 Co-operative Banks 1. State Co-operative Banks 2. District Co-operative Banks 3. Scheduled Urban Cop-operatives Banks 2.1.5 Payment & Settlement System Network 1. Financial market infrastructure 2. Retails payments organization	1. Application should be signed by authorized signatory along with the official seal of the organization 2.Letter of Intent by Head of the Organization / CMD expressing interest to onboard as AUA/KUA 3. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 4.Valid License issued by RBI 5. Certificate of Incorporation 6. Letter of association from ASA 7. Scope Document 8. 2 copies of blank Stamp Papers of requisite denomination as per the state

S.No.	Pre-Qualification Criteria	On-Boarding Documents
	3. Cards payment network 4. ATM networks 5. Pre-paid payment instruments 6. White label ATM operators 7. Instant Money Transfer	9. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria
	In addition	
	2.1.3 Regional Rural Banks	1. Letter of association from PSB
	2.1.4 Co-operative Banks	1. Letter of association from the Center /State government
	2.1.5 Payment & Settlement System Network	1. Board Resolution for making AUA / KUA application
2.2	Regulated by IRDA/PFRDA - Financial Institutions	1. Application should be signed by authorized signatory along with the official seal of the organization 2. Valid License issued by the regulator (IRDA / PFRDA 3.Letter of Intent by Head of the Organization / CMD expressing interest to onboard as AUA/KUA 4. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 5. Certificate of Incorporation 6. Letter of association from ASA 7. Scope Document 8. 2 copies of blank Stamp Papers of requisite denomination as per the state 9. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria 10. Board Resolution for making AUA / KUA application 11. PAN/Service Tax Number/TIN (If any)
2.3	Regulated by TRAI – Telecom	1. Application should be signed by authorized signatory along with the official seal of the organization 2. Letter of Intent by Head of the Organization/CMD expressing interest to

S.No.	Pre-Qualification Criteria	On-Boarding Documents
		onboard as AUA/KUA 3. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 4. Valid License issued by DoT for each circle 5. Certificate of Incorporation 6. Letter of association from ASA 7. Scope Document 8. 2 copies of blank Stamp Papers of requisite denomination as per the state 9. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria 10. Board Resolution for making AUA / KUA application
3	**Other Entities**	
	3.1.1 Company registered in India under the Companies Act 1956 / The Companies Act 2013 3.1.2 Partnership registered under the India Partnership Act 1932 or under the Limited Liability Partnership Act, 2008 3.1.3 Proprietorship Firm 3.1.4 Regulated/Licensed by RBI - 1. Non Banking Financial Companies 2. Non Scheduled Urban Co-operative Banks 3.1.5 Regulated by SEBI - Brokerage firms 3.1.6 Not-for-profit Organizations (under section 25 under The Companies Act 1956) 3.1.7 Academic Institutions / Research and Development Organizations	1. Application should be signed by authorized signatory along with the official seal of the organization 2.Letter of Intent by Head of the Department/CMD/MD/partners/proprietor expressing interest to onboard as AUA/KUA 3. Letter of authority, authorizing the signatory to sign documents on behalf of the organization along with the attested specimen signatures (both initials and full) 4. Letter of association from ASA 5. Copy of Service Tax Number / TIN / PAN 6. Scope Document along with the presentation as mentioned below after this table. 7. List of names of CEO / CFO / Directors / Partners / Trustees / Proprietors / person-in-charge of the agency along with the organization chart. 8. Self-declaration stating that the entity has not been blacklisted by any State Government, Central Government, PSUs, Statutory, Autonomous, or Regulatory body in last three years. 9. Technical declaration as per requested details mentioned in Table Technical Eligibility criteria 10. Financial declaration as per requested details mentioned in Table Financial Eligibility

S.No.	Pre-Qualification Criteria	On-Boarding Documents
	3.1.8 Societies registered under Indian Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The companies Act, 2013 (Sec 8) / Co-operative Society Act 1912 3.1.9 Any other entity which is other than above mentioned categories	criteria
	In addition	
	3.1.1 Company registered in India under the Companies Act 1956 / The Companies Act 2013	1. Extract of AOA and MOA mentioning area of operation pertaining to AUA/KUA 2. Certificate of incorporation 3.Letter of commencement of the Business issued by Ministry of Corporate Affairs (MCA) to a company 4. Board Resolution for making AUA/KUA application
	3.1.2 Partnership registered under the India Partnership Act 1932 or under the Limited Liability Partnership Act, 2008	1. Registered Partnership deed 2. Registration Certificate from Registrar of Firms OR Ministry of Corporate Affairs (MCA), as applicable 3. Certificate of incorporation
	3.1.3 Proprietorship firm	1. Letter of Authorization from proprietor to depute Authorized person for the purpose of AUA/KUA. 2. Valid Business Licenses 3. Legal document issued by the central/state/Local government authority
	3.1.4 Regulated/Licensed by RBI - 1. Non Banking Financial Companies 2. Non Scheduled Urban Co-operative Banks	1. Letter of commencement of the Business issued by Ministry of Corporate Affairs (MCA) to a company 2. Valid License issued by RBI 3. Letter of commencement of the Business issued by Ministry of Corporate Affairs (MCA) to a company 4. Certificate of Incorporation 5. Legal document issued by the central/state/Local government authority

S.No.	Pre-Qualification Criteria	On-Boarding Documents
	3.1.5 Regulated by SEBI - Brokerage firms	1. Valid License issued by SEBI 2. Extract of AOA and MOA mentioning area of operation pertaining to AUA/KUA 4. Certificate of incorporation 5. Legal document issued by the central/state/Local government authority 6. Certified copy of letter of commencement of business issued by Ministry of Corporate Affairs (MCA)
	3.1.6 Not-for-profit Organizations (under section 25 under The Companies Act 1956)	1. Extract of the Constitution mentioning area of operation 2. Legal document issued by the central/state/Local government authority 3. Certified copy of the latest Trust Deed or Society's memorandum of Association or Companies 4. Letter of Authorization from Ministry of Corporate Affairs (MCA)/ Central Government 5. Certificate of incorporation 6. Board Resolution for making AUA/KUA application
	3.1.7 Academic Institutions / Research and Development Organizations	1. Letter from concerned regulatory authority such as UGC, AICTE, MCI, DCI, Education Board, Bar council of India etc 2. Legal document issued by the central/state/Local government authority 3. Certificate of incorporation 4. Board Resolution for making AUA/KUA application
	3.1.8 Societies registered under Indian Societies Registration Act, 1860 / Co-operative Society Act 1912 / Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The companies Act, 2013 (Sec 8)	1. Letter of Authorization from Committee. 2. Constitution Document 3. Certified copy of the latest Trust Deed or Society's memorandum of Association or Companies 4. Registration Certificate from Registrar of Societies OR Ministry of Corporate Affairs (MCA), as applicable 5. Certificate of incorporation 6. Board Resolution for making AUA/KUA application

S.No.	Pre-Qualification Criteria	On-Boarding Documents
	3.1.9 Any other entity which is other than above mentioned categories	1. Extract of AOA and MOA mentioning area of operation pertaining to AUA/KUA 2. Certificate of incorporation 3. Letter of commencement of the Business issued by Ministry of Corporate Affairs (MCA) to a company 4. Legal document issued by the central/state/Local government authority

Presentation details to be submitted by the applicant falling under the category of Other Entities

An organization needs to furnish following details in the form of a document or the presentation:

a. Purpose of Aadhaar integration
b. Benefit of integrating Aadhaar with the service delivery
c. How Aadhaar Authentication/e-KYC services will be integrated
d. Cost benefit Analysis of Aadhaar based service delivery
e. Applying for AUA/KUA/DSDV
f. Modalities (Demographic, Biometric, OTP)
g. Number of Beneficiaries being targeted, expected volume of transactions
h. Sub AUA (If any)
i. Process flow diagram for AUA as well as KUA, if applicable
j. Geographies to be catered
k. Implementation plan (Mandatory to include phase wise dates)
l. Innovative Usage of Aadhaar
m. Social Impact
n. Details of past work experience with supporting documents

***** End of Document *****

Authentication User Agency Application Form

Unique Identification Authority of India

Organization Details	
AUA Organization Name	
AUA Organization Short Name	
Complete Postal Address	
Organization Type *(Select any one option – value to be selected based on AUA eligibility criteria[i] under which the organization qualifies)*	• Central Government Ministry / Department • State Government Ministry / Department • Public Sector Undertaking • Authority constituted under the Central / State Act • Not-for-Profit Company / Special Purpose Organization of national importance • Bank & financial institution • Telecom Service Provider • Others (Pls specify _____)
Industry Sector *(Can select multiple options)*	• Social Sector • Banking & Finance • Telecom • Petroleum & Natural Gas • Hospitality • Education • Health care • Agriculture • Labor & Employment • Others (Pls specify _____)
Contact Details	
Management Point of Contact	
Contact Name	
Designation	
Mobile Number	
Email Address	
Fax Number	

Technical Point of Contact	
Contact Name	
Mobile Number	
Email Address	
Fax Number	
ASA Engagement	
Proposed No. of ASAs for routing authentication request	
Name of ASAs *(An AUA may connect through multiple ASAs)*	
Arrangements in place with ASA?	Yes / No
Propose to have sub-AUAs?	Yes / No / May Be
Authentication Requirements	
Scope Document *(Please attach the document)*	
Usage of authentication *(Can select multiple options)*	• Cleaning existing beneficiary database • Adding new beneficiaries • Confirming beneficiary presence • Financial transactions • Access control • Address verification • Demographic data verification • Attendance management • Accountability tracking • Others (pls specify) _____
Existing beneficiary authentication mechanism *(Can select multiple options)*	• Any ID card • ID card/reference number issued by AUA • Signature • Magnetic / Smart card • Password / PIN • OTP • Others (pls specify) _____

Adoption of federated model *(Select any one option)*	• Will use Aadhaar authentication only • Will use Aadhaar authentication as one factor & another factor from AUA for frequent transactions • Will use Aadhaar authentication on regular basis & AUA authentication for exception handling • Will use Aadhaar authentication on periodic basis & AUA authentication for frequent transactions • Others (pls specify) _____
Target beneficiary population *(Specify the population size in numbers)*	
Expected authentication volume *(Select any one option)*	• Less than 1000 per day • 1000-10,000 per day • 10,000-100,000 per day • More than 100,000 per day
Expected authentication frequency (per beneficiary) *(Select any one option)*	• Daily • Weekly • Fortnightly • Monthly • Quarterly • Half yearly • Annual • Sporadic-frequent • Sporadic-infrequent • One time only
Authentication factors *(Can select multiple options)*	• Personal Identity • Personal Address • OTP • Fingerprint • Iris
Demographic matching options *(Can select multiple options)*	Full / Partial / Local Language
Geographies Catered to *(Please specify states in case multiple states / single state selected)*	• Pan India • Multiple States • State level
Possible locations of Devices/ Terminals *(Can select multiple options)*	Urban / Rural / Semi Urban
Will charge residents for authentication service?	Yes / No / May Be
Will financial transactions be carried out based on authentication?	Yes / No

Readiness Activities	
Aadhaar seeding strategy *(Can select multiple options)*	• Based on enrolment KYR+ data • Part of State Resident Data Hub (SRDH) • Demographic authentication • Biometric authentication • Not Applicable • Others (pls specify) _____
Exception handling *(Can select multiple options)*	• OTP authentication • Operator authentication • AUA's alternate systemic authentication mechanism – smart card, PIN • AUA's alternate physical document based authentication • Other physical document based authentication • Others (pls specify) _____
Fraud monitoring capabilities	Yes / No / In Future
Device form factor *(Can select multiple options)*	• Handheld device • Kiosk • Laptop / PC • Mobile phone • Others (pls specify) _____
Authentication environment *(Can select multiple options)*	• Resident owned devices • Kiosks • Operator assisted • Operator authenticated
How many devices to be deployed *(Select any one option)*	• Less than 500 • 500-5000 • 5000-50,000 More than 50,000
Connectivity supported between AUA & devices *(Can select multiple options)*	• GSM / CDMA • PSTN • Leased line • Others (pls specify) _____
Connectivity supported between AUA & ASA *(Can select multiple options)*	• VPN • Leased line • Others (pls specify) _____
Agree to UIDAI contract terms & conditions?	Yes / No
Sent documents supporting AUA eligibility criteria and other requirements to UIDAI?	Yes / No

Authentication User Agency Application Form

Unique Identification Authority of India

Submitted By *(from AUA organization)*	**Approved By** *(from UIDAI)*
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Organization: _____	Organization: _____
Date: _____	Date: _____

Unique Identification Authority of India

Go-Live Checklist*		
1	AUA has established infrastructure for digital signature	☐
2	AUA data logging for Authentication Audit trail being provisioned	☐
3	AUA has obtained UIDAI production public key for encryption from UIDAI developer portal	☐
4	AUA has performed end-to-end testing with UIDAIs pre-production environment in collaboration with Authentication Service Agency (ASA)	☐
5	AUA is ready to deploy devices with STQC certified sensor-extractor, if using biometric authentication	☐
6	AUA has integrated Best Finger Detection (BFD) functionality in client application, if using biometric fingerprint authentication	☐
7	AUA has implemented two finger authentication in client application, if using biometric fingerprint authentication	☐
8	Resident consent process to obtain consent is ready to be deployed	☐
9	Obtained certificate from an information systems auditor certified by a recognized body for compliance to UIDAIs standards and specifications	☐

*All the above items are mandatory and need to be completed before submitting for go live approval to UIDAI.

For additional information on the above checklist items please refer UIDAI website http://uidai.gov.in/auth.html

Please note that production AUA code and license key will be provided post UIDAI approval of this checklist.

AUA hereby confirms compliance to the current standards and specifications as published by UIDAI.

Submitted By *(from AUA organization)*

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Approved By *(from UIDAI)*

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

[i] Refer Section 2.4.2 of Aadhaar Authentication Operating Model

AUTHENTICATION USER AGENCY AGREEMENT

This **AUTHENTICATION USER AGENCY AGREEMENT** ("**Agreement**") is made as of this _____ day of _____, and year _____, by and between:

1. The President of India acting through ___Name, _____Designation _____ _____(**UNIQUE IDENTIFICATION AUTHORITY OF INDIA**, having its registered office at 3rd Floor, Tower II, Jeevan Bharati Building, Connaught Circus, New Delhi-110001 (hereinafter called the "**UIDAI**", which expression shall unless excluded by or repugnant to the context be deemed to include his successor in office, administrators and permitted assigns), OF THE FIRST PART.

AND

2. _____
_____
_____
_____,
having its registered address at
_____
_____
_____ (hereinafter referred to as "**Authentication User Agency**", which expression shall unless repugnant to the context or meaning thereof, include its successors and permitted assigns), OF THE SECOND PART.

WHEREAS:

A. UIDAI has been set up with the mandate of issuing unique identification numbers, i.e., "Aadhaar Numbers" to the residents of India, based on their biometric and demographic information.

B. The Aadhaar Number and Personal Identity Information (PID) of the Aadhaar Holder can be authenticated through an online mechanism provided by UIDAI for this purpose, which authentication mechanism is provided by UIDAI free of charge till **31st December, 2016**, where after the same may or may not be charged for, at the sole discretion of UIDAI.

C. The Authentication User Agency is desirous of using the Aadhaar Authentication Services provided by UIDAI, through an Authentication Service Agency, so as to provide Aadhaar Enabled Services to its beneficiaries, clients and customers and has approached UIDAI, by way of an application, for appointment as an Authentication User Agency.

D. The Authentication User Agency is aware of, and understands, the fact that UIDAI's operation of the Aadhaar Authentication Services is subject to limitations posed by technology, and UIDAI does not represent and warrant the same to be defect free.

E. The Authentication User Agency is aware of, and understands that the Aadhaar Authentication Services are provided on an 'as is' basis, without any express or implied warranties in respect thereof, and UIDAI does not assume any responsibility or liability for any damage, whether direct, indirect, incidental or consequential, arising as a result of the use of the Aadhaar Authentication Services except the damages which solely arise out of False acceptance by UIDAI biometric authentication services.

F. UIDAI has evaluated the application of the Authentication User Agency and has granted recognition to and approval for appointment of the Authentication User Agency as an Authentication User Agency for providing Aadhaar Enabled Services.

G. UIDAI has further evaluated the application of the Authentication User Agency and has granted recognition to and approval for appointment/empanelment of the Authentication User Agency as a KYC User Agency (KUA) for the e-KYC service, subject to annexure 1 duly signed by UIDAI and the Authentication User Agency. In such a case Authentication User Agency is also referred to as KYC User Agency (KUA) and references to Authentication User Agency also mean KYC User Agency and similarly Authentication Service Agency also mean KYC Service Agency.

NOW THEREFORE, in consideration of the mutual covenants and promises set forth herein and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby covenant and agree and this Agreement witnesseth as follows:

1. DEFINITIONS & INTERPRETATION

"Aadhaar Authentication Services" shall mean the authentication services provided by UIDAI and used by Authentication User Agency where the personal identity information of/data of an Aadhaar-holder (who is a beneficiary, customer, employee or associate of the Authentication User Agency is matched with their personal identity information/data that is stored in the UIDAI's Central Identity Data Repository in order to provide Aadhaar enabled services to such Aadhaar holder. The Authentication User Agency shall avail Aadhaar authentication service by establishing a connection with UIDAI's Central Identity Data Repository, through an Authentication Service Agency. The Aadhaar authentication services shall be provided in the manner and as per matrix and conditions specified in Schedule I.

"Aadhaar Enabled Services" shall mean services provided by an Authentication User Agency to Aadhaar Holder, using the Aadhaar Authentication Services of UIDAI.

"Aadhaar Holder" shall mean an individual who holds an Aadhaar Number.

"Aadhaar Number" shall mean the unique identification number issued to resident by UIDAI.

"**Agreement**" shall mean this agreement executed between the Parties, alongwith its schedules, annexures and exhibits, if any, and all instruments supplemental to or amending, modifying or confirming this agreement in accordance with the provisions of this agreement, if any, in each case as they may be supplemented or amended from time to time.

"Authentication Device" shall mean a terminal or device from where the Authentication User Agency carries out its service/business functions and interacts with Aadhaar Holders, by seeking authentication of Aadhaar Holders identity to enable the Authentication User Agency's business function.

"Authentication Service Agency" shall mean an entity providing compliant secured network connectivity to the UIDAI and the Authentication User Agency for enabling Aadhaar Authentication Services as separate agreements entered into between the entity and UIDAI and Authentication User Agency respectively.

"Biometric Information" shall mean ten finger prints and iris image, captured by UIDAI, as a part of the enrolment process for issuance of Aadhaar Number.

"Business Day" shall mean any day other than a Saturday, Sunday or official public holiday in India.

"Central Identity Data Repository (CIDR)" means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

"Confidential Information" shall mean any information which is considered confidential in terms of Clause 9 of this Agreement and shall include, but not limited to, information such as Aadhaar Number, name, address, age, date of birth, relationships and other demographic information, as also, biometric information such as finger print and iris scan of a resident.

"e-KYC" shall mean the transfer of demographic data (such as Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph collected by UIDAI in the form of a digitally signed XML document to an Authentication User Agency, through an Authentication Service Agency, based on resident authorization received by UIDAI in the form of successful biometric or OTP-based Aadhaar authentication.

"False Accept" shall be referred to a accept transaction where a system identifies a biometric as genuine (while, in reality it belongs to some other individual) or will fail to reject an impostor biometric. Imposter can be defined as someone who intentionally or unintentionally is presenting his/her biometric against someone else's Aadhaar number.

"KYC User Agency" shall mean Authentication User Agency that is eligible for the e-KYC service.

"KYC Service Agency" shall mean Authentication Service Agency that is eligible to

provide access to the e-KYC service through their network.

"Law(s)" shall mean all applicable laws, by-laws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any governmental authority or person acting under the authority of any governmental authority, whether in effect or which may come into effect in the future.

"OTP" shall mean one time password sent to the Aadhaar holder's cell phone for the purpose of authentication.

"Party" refers individually to UIDAI and the Authentication User Agency and

"**Parties**" refer collectively to UIDAI and Authentication User Agency.

"Personal Identity Data (PID)" refers to Aadhaar-based Personal Identity Data/ Information including biometric and demographic information as well as the OTP used for Authentication

"Standards" shall mean the standards issued by UIDAI with regard to matters covered by this Agreement, and sole right of interpretation whereof shall rest with UIDAI at all times.
"**Sub-AUA**" shall mean an entity appointed by the Authentication User Agency under this agreement to access Aadhaar authentication services through the Authentication User Agency.

"Term" shall mean the duration specified in Clause 10.

"Third Party" shall mean any party who is not a Party.

1.2 Interpretation

1.2.1 In this Agreement, unless the context requires otherwise:

(i) reference to singular includes a reference to the plural and vice versa;

(ii) reference to any gender includes a reference to all other genders;

(iii) reference to an individual shall include his legal representative, successor, legal heir, executor and administrator;

(iv) reference to statutory provisions shall be construed as meaning and including references also to any amendment or re-enactment (whether before or after the date of this Agreement) for the time being in force and to all statutory instruments or orders made

pursuant to statutory provisions;

(v) references to any statute or regulation made using a commonly used abbreviation, shall be construed as a reference to the title of the statute or regulation;

(vi) references to any Article, Clause, Section, Schedule or Annexure, if any, shall be deemed to be a reference to an Article, Clause, Section, Schedule or Annexure of or to this Agreement.

1.2.2 Clause headings in this Agreement are inserted for convenience only and shall not be used in its interpretation.

1.2.3 When any number of days is prescribed in this Agreement, the same shall be reckoned exclusively of the first and inclusively of the last day unless the last day does not fall on a Business Day, in which case the last day shall be the next succeeding day which is a Business Day.

1.2.4 If any provision in this Agreement is a substantive provision conferring rights or imposing obligations on anyone, effect shall be given to it as if it were a substantive provision in the body of this Agreement.

1.2.5 Any word or phrase defined in the body of this Agreement shall have the meaning assigned to it in such definition throughout this Agreement unless the contrary is expressly stated or the contrary clearly appears from the context.

1.2.6 The rule of construction, if any, that a contract shall be interpreted against the party responsible for the drafting and preparation thereof shall not apply.

1.2.7 Reference to days, months or years in this Agreement shall be a reference to calendar days, months or years, as the case may be, unless the contrary is expressly stated or clearly appears from the context.

1.2.8 Reference to any agreement, deed, document, instrument, rule, regulation, notification, statute or the like shall mean a reference to the same, as may have been duly amended, modified or replaced. For the avoidance of doubt, a document shall be construed as amended, modified or replaced only if such amendment, modification or replacement is executed in compliance with the provisions of such document(s).

2. APPOINTMENT OF AUTHENTICATION USER AGENCY

2.1 UIDAI hereby appoints the Authentication User Agency, as an Agency authorised to send requests for authenticating PID of Aadhaar Holder(s), subject to the terms and conditions of this Agreement.

2.2 The Authentication User Agency hereby unequivocally accepts its appointment as an Authentication User Agency, for providing Aadhaar Enabled Services to Aadhaar Holder(s), in terms of clause 2.1 above.

3. TERMS AND CONDITIONS OF APPOINTMENT OF AUTHENTICATION USER AGENCY

3.1 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 authentication related 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 information systems auditor certified by a 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 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 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.

3.2 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.

3.3 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 for the purposes set out in Schedule-II

to this Agreement, and for no other purposes. In the event, the Authentication User Agency is desirous of using Aadhaar Authentication Services, for new and additional services/business functions without compromising or violating requirements specified by UIDAI with regard to network specifications, security etc., from time to time, it shall inform UIDAI in this regard

3.4 It is hereby expressly agreed between the parties that in cases where the Authentication User Agency or its Sub AUA forwards an authentication request to the Central Identity Data Repository, through an Authentication Service Agency, and in the event of an Aadhaar authentication failure for whatever reasons, the Authentication User Agency may invoke other means of Identity authentication for service provision to the Aadhaar Holder, and the Authentication User Agency or its Sub AUA shall bear full responsibility for any decision taken in this regard and UIDAI shall have no role in this regard.

3.5 The Authentication User Agency hereby unequivocally agrees that all backend infrastructure, such as servers, databases etc., required specifically for the purpose of Aadhaar authentication shall be based in the territory of India.

3.6 The Authentication User Agency hereby unequivocally agrees that the use of the Aadhaar Authentication Services by it for providing Aadhaar Enabled Services to Aadhaar Holder(s) and the Aadhaar Authentication Services shall not, in any manner, whether direct or indirect, be used for purposes that are anti-government or anti-State or discriminatory or related to money laundering or in contravention of any laws applicable in India.

4. OBLIGATIONS OF UIDAI

4.1 UIDAI shall:

a) determine rules and frameworks regarding the usage of Aadhaar Number and Aadhaar Identity Data;

b) register/certify/approve, by itself or through approved independent certification agencies, all the applications & devices, such as applications driving the authentication systems in the Authentication User Agency's and Sub AUA's systems, that will be used by the Authentication User Agency;

c) determine and prescribe Standards and specifications for transmission of Aadhaar Identity Data for the purposes of Aadhaar Authentication Services and Aadhaar Enabled Services;

d) determine and prescribe Standards to ensure the confidentiality, privacy and security of Aadhaar Identity Data;

e) prescribe other Standards and specifications that UIDAI may deem necessary, in its sole judgment, for providing Aadhaar Authentication Services and Aadhaar Enabled Services;

4.2 Notwithstanding anything contained in Clauses 4.1 above, it is hereby clearly understood by the Parties that UIDAI shall have no responsibility or liability in relation to failures that may take place during the Aadhaar based authentication process, including but not limited to, failures as a result of, false reject, network or connectivity failure, device failure, possible down time at Central Identities Data Repository, etc.

5. OBLIGATIONS OF THE AUTHENTICATION USER AGENCY

5.1 The Authentication User Agency shall, for every service/business function for which it is desirous of using Aadhaar Authentication Services, chooses suitable authentication type, for each particular service, from Aadhaar Authentication package Framework provided by UIDAI from time to time, which indicates the identity credentials (PID) to be sought from the Aadhaar Holder, who is seeking to access the specific service/business function(s). For avoidance of doubt, it is hereby expressly stated that the choice of authentication type(s), in the manner provided above, shall be the sole decision of the Authentication User Agency, and no other entity, including UIDAI, Authentication Service Agency and Aadhaar Holder shall have any role in this decision of Authentication User Agency.

5.2 The Authentication User Agency shall obtain a consent from the Aadhaar holder, for using the Aadhaar number and Biometric information for providing the Aadhaar Authentication Service

5.3 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, with the Central Identities Data Repository, established by UIDAI that contains all Aadhaar Identity Data, in compliance with all the specifications and standards prescribed by UIDAI, from time to time. The Authentication User Agency assumes complete responsibility with regard to its network connectivity with an Authentication Service Agency. And UIDAI shall have no responsibility in this regard. Provided where the Authentication User Agency has entered into another agreement with the UIDAI to act as an Authentication Service Agency, such an Authentication User agency need not engage another Authentication Service Agency.

5.4 The Authentication User Agency shall establish and maintain necessary

authentication related operations, including their own systems, processes, infrastructure, technology, security, etc., which may be necessary for providing Aadhaar Enabled Services, in compliance with standards and specifications, issued by UIDAI from time to time.

5.5 The Authentication User Agency shall ensure that the network connectivity between authentication devices and the Central Identities Data Repository, used for sending their authentication requests is in compliance with the standards and specifications issued by UIDAI from time to time. The Authentication User Agency shall build and maintain the connectivity between authentication devices and the Authentication Service Agency's systems either by itself, or by outsourcing it to a service provider. The Authentication User Agency shall work with the Authentication Service Agency in ensuring the compliance of the connectivity between the Authentication Service Agency and Central Identities Data Repository.

5.6 The Authentication User Agency shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners) which are duly registered with/approved/certified by UIDAI or an agency appointed by UIDAI for this purpose. The Authentication User Agency understands the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which confirm to the authentication type adopted by the Authentication User Agency, and UIDAI shall have no role to play in this regard, and shall have no liability or responsibility in this respect.

5.7 The Authentication User Agency shall install necessary Authentication Devices and other Information Technology devices along with device installation and maintenance kits, and the devices shall comply with specifications and standards prescribed by UIDAI from time to time. The Authentication User Agency shall ensure that the applications driving the authentication devices are duly registered with/approved/certified by UIDAI. The Authentication User Agency assumes complete responsibility for ensuring that the processes, procedures, systems and infrastructure at Authentication Device are in compliance with standards and specifications issued by UIDAI from time to time.

5.8 It is hereby expressly agreed between the Parties that in the event Authentication User Agency's federated authentication system includes Aadhaar authentication as well as the Authentication User Agency's local authentication system, the Authentication User Agency shall integrate their authentication systems with Aadhaar authentication system in compliance with standards and specifications issued by UIDAI from time to time.

5.9 The Authentication User Agency shall keep UIDAI informed of the Sub AUAs with whom they have entered into agreements and shall duly register them in the manner prescribed by UIDAI from time to time. The AUA shall issue a Sub AUA code to identify each Sub AUA and shall include the Sub AUA code in all authentication requests originating from that Sub AUA which it forwards to CIDR for authentication. The AUA shall keep the UIDAI informed of all Sub AUA codes that it issues. The Authentication User Agency shall ensure that the Sub AUAs comply with standards and protocols laid out by UIDAI from time to time. The Authentication User Agency understands that it shall be responsible for all authentication requests originating from the Sub AUA and routed through the Authentication User Agency

5.10 The Authentication User Agency shall keep UIDAI informed of the list of Authentication Service Agency(ies) with whom they have any agreement(s), in the manner prescribed by UIDAI from time to time. The Authentication User Agency shall inform UIDAI, forthwith, all relevant information pertaining to any agreement that it may enter into with an Authentication Service Agency and any subsequent modifications thereto, if any. Authentication User agency is obligated to send the agreement entered with Authentication Service Agency immediately upon request from UIDAI. In the event the Authentication User Agency disengages with an Authentication Service Agency, the fact of disengagement shall be communicated to UIDAI, by the Authentication User Agency, within such period as may be prescribed by UIDAI from the date of disengagement.

5.11 The Authentication User Agency shall ensure that the persons employed by it for providing Aadhaar Enabled Services and for maintaining necessary systems, infrastructure, processes, etc. in this regard, possess requisite qualifications for undertaking such works. The Authentication User Agency shall be responsible for ensuring that, in case Authentication Devices are operated by its own or its agents personnel, such personnel are suitably and adequately trained to conduct Aadhaar Enabled Services, in compliance with specifications and standards prescribed by UIDAI from time to time.

5.12 The Authentication User Agency shall, at all times, comply with standards, directions, specifications, etc. issued by UIDAI, in terms of network and other Information Technology infrastructure, processes, procedures, etc. for the purposes of availing Authentication services provided by UIDAI. The Authentication User Agency shall be further responsible, at all times, for compliance with specification issued by UIDAI, from time to time, with respect to all authentication related aspects. In the event the Authentication User Agency outsources part(s) of its operations to other

entities, the ultimate responsibility for the results of authentication related operations shall lie with the Authentication User Agency.

5.13 The Authentication User Agency shall, at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed there under, from time to time, in so far the same has application to its operations in accordance with this Agreement, and also with all other Laws rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security and management, data storage, sharing and data protection, as also with the National Identification Authority of India Bill, as and when the same is enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device.

5.14 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 recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the audit report should be shared with UIDAI upon request. In addition to the above, UIDAI may choose to, in its sole discretion, audit the AUA's operations and systems in terms of this Agreement by itself or through an 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. "The Authentication User Agency unequivocally agrees to provide full co-operation 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,

5.15 The Authentication User Agency shall monitor the operations of its Authentication Device, on a periodic basis, for compliance with the terms and conditions contained in this Agreement or with standards, directions, specifications, etc. issued and communicated by UIDAI, in this regard, from time to time.

5.16 The Authentication User Agency shall maintain logs of all authentication transactions processed by it, capturing the complete details of the authentication transaction, such as the Aadhaar number against which authentication is sought, authentication package, date and timestamp, etc. as prescribed by UIDAI from time to time but shall not, in any event,

capture the PID information and shall retain the same for a duration, specified by UIDAI from time to time. The Authentication User Agency understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need-basis, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

5.17 In case of any investigations around authentication related fraud(s) or dispute (s), the Authentication User Agency shall extend full cooperation to UIDAI, and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource/information, etc. of or pertaining to its Authentication Device.

5.18 The Authentication User Agency, where ever applicable, shall be responsible for identifying exception-handling mechanisms in the event of failure of Aadhaar Authentication Services.

5.19 The authentication charges, for providing Aadhaar Enabled Services by the Authentication User Agency to its customers, shall be evolved by the Authentication User Agency and UIDAI shall have no say in this respect, for the time being, however, UIDAI's right to prescribe a different mechanism in this respect, in the future, shall be deemed to have been reserved.

5.20 The Authentication User Agency unequivocally agrees that all devices and applications used by it in running its Aadhaar authentication operations shall be duly certified/approved by UIDAI or an agency appointed/ approved by UIDAI (as and when UIDAI creates a certification mechanism for certifying Aadhaar enabled application). In the event the already certified/approved applications employed by the Authentication User Agency undergo modifications, the Authentication User Agency shall deploy the modified applications only after renewed certification/approval from UIDAI.

5.21 The Authentication User Agency agrees to incorporate and adopt standards, specifications and other terms and conditions as prescribed by UIDAI from time to time, in its agreement with the ASA for the purpose of availing Authentication services of UIDAI.

5.22 Authentication User Agency hereby agrees to inform UIDAI of any misuse of Aadhaar data or any compromise of Aadhaar related data or systems within their network.

6. REPRESENTATIONS AND WARRANTIES

6.1 UIDAI represents and warrants to the Authentication User Agency that:

(a) UIDAI is an authority set up by the Planning Commission, Government of India;

(b) UIDAI has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;

(c) this Agreement has been validly executed by UIDAI and constitutes a valid agreement binding on UIDAI and enforceable in accordance with the laws of India;

6.2 The Authentication User Agency represents and warrants to UIDAI that:

(a) the Authentication User Agency is an entity legally constituted and validly existing under the laws of India;

(b) the Authentication User Agency has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;

(c) this Agreement has been validly executed by the Authentication User Agency and constitutes a valid agreement binding on the Authentication User Agency and enforceable in accordance with the laws of India.

7. INTELLECTUAL PROPERTY

7.1 The Authentication User Agency is aware that "Aadhaar" is the intellectual property of UIDAI and the Authentication User Agency understands that any unauthorized reproduction of the same constitutes infringement and may be subject to penalties, both civil and criminal.

7.2 It is hereby mutually agreed between the Parties that the Authentication User Agency shall have a non-exclusive right to use the Aadhaar name and logo and to represent itself as an entity providing Aadhaar Enabled Services to Aadhaar Holder(s), subject to the condition that all rights, title and interest, including intellectual property rights, in the Aadhaar name and logo shall vest, at all times, either during the operation of this Agreement or otherwise, in UIDAI.

7.3 The Authentication User Agency hereby unequivocally agrees that it shall use the Aadhaar name and logo, without any modification, in its promotional, educational and informational literature, for the duration of

this Agreement.

7.4 The Authentication User Agency hereby unequivocally agrees that it shall not authorize any other entity or individual to use the Aadhaar name and logo, except with the prior written permission of UIDAI.

7.5 The Authentication User Agency hereby unequivocally agrees that upon becoming aware of unauthorized use, copy, infringement or misuse of the Aadhaar name and/or logo, and any rights, title and interest therein, including intellectual property rights, it shall notify UIDAI about such unauthorized use forthwith. At the request and cost of UIDAI, the Authentication User Agency shall take part in or give assistance in respect of any legal proceedings and execute any documents and do any things reasonably necessary to protect the rights, title and interest of UIDAI, including intellectual property rights, in respect of the Aadhaar name and logo.

8. INDEMNITY AND LIMITATION OF LIABILITY

8.1 The Authentication User Agency understands that the use of Aadhaar Authentication Services by the Authentication User Agency does not result in incurring of any liability by UIDAI whatsoever. The Authentication User Agency alone is responsible for the proper and judicious use of the Aadhaar Authentication Services. UIDAI shall not, in any case, be held responsible for damage and/or harm, direct or indirect, material or immaterial, or of any nature whatsoever, arising from any unavailability of the Aadhaar Authentication Services or its use by the Authentication User Agency except the damages which solely arising out of false acceptance by UIDAI biometric authentication services.

8.2 It is hereby mutually agreed between the Parties that UIDAI shall not be liable for any unauthorized transactions occurring through the use of Aadhaar Authentication Services and the Authentication User Agency hereby fully indemnifies and holds UIDAI harmless against any action, suit, proceeding initiated against it or any loss, cost or damage incurred by it as a result thereof.

8.3 Without prejudice to generality of the above, the Authentication User Agency shall indemnify and keep UIDAI harmless and indemnified from and against all claims, liabilities, losses and incurred costs, fines, penalties, expenses, taxes, assessment, punitive damages, fees (including advocate's/ attorney's fee), liabilities (including any investigative, legal and other expenses incurred in connection with, and any amounts paid in settlement of, any pending or threatened legal action or proceeding), judgments,

awards, assessments, obligations, damages, etc., which UIDAI may suffer or incur arising out of, or in connection with:

a) any act, neglect, default or omission on the part of the Authentication User Agency, its subsidiaries or any person associated with the Authentication User Agency, including but not limited to liabilities arising from non compliance of Standards and Regulations prescribed by UIDAI, from time to time, unauthorized use or disclosure of Confidential Information and failure to comply with data protection and storage requirements, as prescribed by UIDAI, from time to time;
b) any breach by the Authentication User Agency of the terms and conditions or its appointment or its obligations under this Agreement;
c) any breach by the Authentication User Agency of its obligations under any Law(s) or contract, etc;
d) default or omission on the part of the Authentication User Agency to

follow statutory instructions and guidelines issued by the Government of India, National Identification Authority of India (as and when setup) and any other governmental authority.

8.4 In the event of a Third Party bringing a claim or action against UIDAI, as a consequence of the use of Aadhaar Authentication Services by the Authentication User Agency or its Sub AUA, the Authentication User Agency shall:

a) defend and / or to assist UIDAI in defending, at the Authentication User Agency's cost, such claims or actions, either in a legal proceeding or otherwise;

b) indemnify UIDAI and keep UIDAI indemnified and harmless, at all times, against all actions, claims, demands, costs, charges and expenses arising out of or incurred by reason of any infringement of intellectual property rights of any Third Party in connection with the use of the Aadhaar Authentication Services, irrespective of whether or not UIDAI incurs any liability in this regard by virtue of any judgment of a court of competent jurisdiction.

8.5 The Authentication User Agency is aware of, and understands, the fact that UIDAI's operation of the Aadhaar Authentication Services is not completely free from defect, and UIDAI does not represent and warrant the same to be defect free. Unless otherwise expressly specified in writing, the Aadhaar

Authentication Services are provided on an 'as is' basis, without any express or implied warranties in respect thereof. It is hereby mutually agreed between the Parties that under no circumstances shall UIDAI be liable for any damages whatsoever, whether such damages are direct, indirect, incidental consequential and irrespective of whether any claim is based on loss of revenue, interruption of business or any loss of any character or nature whatsoever and whether sustained by the Authentication User Agency or by any other person, as a result of the operation of this Agreement or otherwise except the damages which solely arising out of false acceptance by UIDAI biometric authentication services.

8.6 The maximum liability for which UIDAI may be held responsible in respect of a false acceptance shall be restricted to the amount of that transaction or the actual unrecovered direct loss to the Authentication User Agency or maximum amount of liability fixed by UIDAI time to time , whichever is less Provided that:

a) The Authentication User Agency actually suffers a direct loss of the said amount, and there being no recourse of recovery thereof from the incorrect beneficiary account or

b) Where recourse does exist, it would be incumbent on the Authentication User Agency to diligently pursue recovery and where recovery either partial or full, has been effected, the liability of UIDAI would stand reduced by that extent.

The liability as mentioned above will be subject to the Compliance by Authentication User Agency of all the procedures, standards and specification as prescribed by UIDAI from time to time in this regard.

8.7 It is hereby mutually agreed that this Clause 8 shall survive the termination of this Agreement.

9. CONFIDENTIALITY, DATA PROTECTION, SECURITY AND USE OF INFORMATION

9.1 The Authentication User Agency and all its Sub AUAs 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 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.

9.2 The Authentication User Agency shall use the Confidential Information strictly for the purposes of authentication of the Aadhaar Holder, and for providing Aadhaar Enabled Services, in accordance with this Agreement. The Authentication User Agency shall ensure compliance with all applicable laws and regulations including but not limited to regulations on data protection under the Information Technology Act, 2008 when collecting information from residents for their business purposes.

9.3 The Authentication User Agency shall scrutinize the data collected by it, while processing authentication requests, on a periodic basis, and shall preserve such data collected in relation to an authentication request until such as may be prescribed by UIDAI from time to time.

9.4 The Authentication User Agency is prohibited from storing any PID in their data base or in any storage device of any nature whatsoever including Authentication Device or in any machine, device or instrument of any kind whatsoever, removable storage devices or in physical form, at point in time.

9.5 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 operation of this Agreement, is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof.

9.6 It is hereby mutually agreed between the parties that UIDAI assumes no responsibility or liability for any action or inaction, use or misuse of the Confidential Information and other data in the control of the Authentication User Agency. The Authentication User Agency agrees and acknowledges that any loss, damage, liability caused or suffered by the Authentication User Agency due to disclosure of all information of confidential nature shall be borne by Authentication User Agency without transferring any liability or responsibility towards UIDAI.

9.7 It is hereby mutually agreed that this Clause 9 shall survive the termination of this Agreement.

10. TERM, TERMINATION AND CONSEQUENCES

10.1 This Agreement shall be in force for a period of _____ years from the Effective Date, unless renewed by mutual consent, in writing, of the Parties, prior to expiry of this Agreement, upon such terms and conditions as may be mutually agreed between the Parties.

10.2 UIDAI shall have the right to terminate this Agreement by giving thirty (30) days notice, in writing, prior to expiry of the Term, without any protest or demur from the Authentication User Agency, in the event of the Authentication User Agency:

a) fails to comply with the Standards or the decision and directions issued by UIDAI, from time to time, with regard to the interpretation and enforcement of the Standards;

b) is in breach of its obligations under this Agreement;

c) uses the Aadhaar Authentication Services for any other purpose than those specified in Schedule-II of this Agreement;

d) is in liquidation, or if a receiver has been appointed in respect of the Authentication User Agency or the Authentication User Agency becomes subject to any form of insolvency administration or files for voluntary liquidation.

e) In case the AUA is also an ASA, termination of the ASA agreement with UIDAI will automatically terminate this agreement.

10.3 The Authentication User Agency shall have no right to compensation for termination of this Agreement by UIDAI, in pursuance of clauses 10.2 above.

10.4 The termination of this Agreement by UIDAI, in pursuance of clauses 10.2 above, shall result in automatic cancellation of the registration of the Authentication User Agency, granted by UIDAI, without any notification, in this regard, to the Authentication User Agency.

10.5 The Authentication User Agency may terminate this agreement by giving 30 days' notice in writing to the UIDAI.

10.6 Upon termination of this Agreement, the Authentication User Agency shall, forthwith, cease to use the Aadhaar name and logo for any purposes, and in any form, whatsoever.

11. FORCE MAJEURE

11.1 The Parties agree that neither of them shall be liable to the other for any loss, delay, damage or other casualty suffered or incurred by the other owing to earthquakes, floods, fires, explosions, acts of God, acts of State, war, terrorism, action of any governmental authority or any other cause,

which is beyond the reasonable control of that Party ("**Force Majeure**") and any failure or delay by any Party in the performance of any of its obligations under this Agreement owing to one or more of the foregoing causes shall not be considered as a breach of any of its obligations under this Agreement. The Parties however agree that any financial failure or non-performance of any financial obligations or covenants of the Parties shall not constitute Force Majeure.

11.2 The Party claiming benefit of Force Majeure shall however not be entitled to the same unless it has intimated the other Party of the occurrence of such event within a period of seventy two (72) hours from the occurrence of such Force Majeure event indicating therein the steps that it is taking or intending to take to mitigate the effect of such Force Majeure on the performance of his obligations under this Agreement.

11.3 In the event, the Force Majeure event continues for a period of more than ninety (90) days, the Party shall renegotiate this Agreement in good faith and if the Parties do not reach any consensus on modifications to this Agreement within a period of one hundred twenty (120) days from the date of occurrence of the Force Majeure event, this Agreement shall automatically stand terminated on such date.

12. GOVERNING LAW AND DISPUTE RESOLUTION

12.1 This Agreement shall, in all respects, be governed by, and construed in accordance with the laws of India.

12.2 Any dispute of whatever nature, which arises out of, in relation to, or otherwise connected with:

(a) the interpretation or effect of;

(b) the validity, enforceability or rectification (whether in whole or in part) of;

(c) the respective rights or obligations of the Parties; and/or

(d) a breach (including a breach of any representation and warranty and/or the materiality thereof and/or the amount of compensation payable in order to remedy such breach and/or the breach or failure to comply with any covenants or undertakings contained herein) or the termination or cancellation of, this Agreement or in regard to whether either Party have unreasonably withheld its approval or

consent under circumstances in which it may not do so; shall be dealt with in accordance with succeeding provisions of this Clause 12.

(All disputes arising out of reasons mentioned herein-above shall be collectively referred to hereinafter as a "**Dispute(s)**").

12.3 All Disputes shall at the first instance be resolved through good faith negotiations, which negotiations shall begin promptly after a Party has delivered to the other Party a written request for such consultation.

12.4 If the Parties are unable to resolve the Dispute in question within thirty (30) days of the commencement of negotiations in terms of Clause 12.3, then the Dispute shall, unless the Parties otherwise agree in writing, be referred for determination in accordance with the remaining provisions of this Clause 12.

12.5 The Dispute shall be referred to arbitration in accordance with the provisions of the (Indian) Arbitration and Conciliation Act, 1996.

12.6 The venue for arbitration shall be New Delhi, India and the language used in the arbitral proceedings shall be English.

12.7 The reference shall be referred to arbitration of an Arbitrator, to be nominated by Secretary, Department of Legal Affairs ("Law Secretary"). The award of the Arbitrator shall be binding upon Parties to the dispute.

12.8 The decision of the Arbitrator appointed to deal with such matters shall be accepted by the Parties as final and binding.

12.9 The Parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration.

12.10 The Parties shall use their best endeavors to procure that the decision of the Arbitrators shall be given within a period of six (6) months or soon thereafter as is possible after it has been demanded.

12.11 This Clause 12 is severable from the rest of this Agreement and shall remain in effect even if this Agreement is terminated for any reason.

12.12 The Courts in New Delhi, India shall have exclusive jurisdiction in relation to this Agreement, including this Clause 12.

12.13 All fees and costs pertaining to arbitration proceedings shall be borne equally by the Parties.

12.14 All other fees and costs incurred by the Parties shall be borne by the respective Parties.

13. GENERAL

13.1 Notices

Any notice, direction or other documentation required or remitted to be given hereunder shall be in writing and may only be given by personal delivery, international courier, electronic mail or facsimile (with confirmation received) at the addresses hereinafter set forth:

(i) For UIDAI :

Address : 3rd Floor, Tower II,
Jeevan Bharati Building
Connaught Circus
New Delhi-110001

Attention : _____
Fax No. : 011 - 23752679

(ii) For the Authentication User Agency :

Address : _____
_____
_____

Attention : _____
Fax No. : _____

13.2 Further Assurances

The Parties hereto shall sign such further and other papers, cause such meetings to be held, resolutions passed and bylaws enacted, exercise their vote and influence, do and perform and cause to be done and performed such further and other acts and things as may be necessary or desirable in order to give full effect to this Agreement and every part hereof.

13.3 No Waiver

No failure by a Party to take any action with respect to a breach of this Agreement or a default by any other Party shall constitute a waiver of the former Party's right to enforce any provision of this Agreement or to take action with respect to such breach or default or any subsequent breach or default. Waiver by any Party of any breach or failure to comply with any provision of this Agreement by a Party shall not be construed as, or constitute, a continuing waiver of such provision, or a waiver of any other breach of or failure to comply with any other provision of this Agreement, unless any such waiver has been consented to by the other Party in writing.

13.4 Severability

If any Clause or part thereof, of this Agreement or any agreement or document appended hereto or made a part hereof is rendered invalid, ruled illegal by any court of competent jurisdiction, or unenforceable under present or future Laws effective during the term of this Agreement, then it is the intention of the Parties that the remainder of the Agreement, or any agreement or document appended hereto or made a part hereof, shall not be affected thereby unless the deletion of such provision shall cause this Agreement to become materially adverse to any Party in which case the Parties shall negotiate in good faith such changes to the Agreement, or enter into suitable amendatory or supplementary agreements, as will best preserve for the Parties the benefits and obligations under such provision.

13.5 Enurement

Upon receipt of consent from UIDAI as required in Clause 3.2 this Agreement will enure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns.

13.6 Counterparts

This Agreement may be executed in one or more counterparts, all of which shall be read and construed as one document and any facsimile signature hereto shall be deemed to be an original signature.

13.7 Independent Legal Advice

Each of the Parties acknowledges that it has received independent legal advice regarding the terms of this Agreement.

13.8 Entire Agreement

This Agreement constitutes the entire agreement between the Parties. There are not and will not be any verbal statements, agreements, assurances, representations and warranties or undertakings among the Parties and this Agreement may not be amended or modified in any respect except by written instrument signed by the Parties.

13.9 Independence of the Parties with respect of each other

Each of the Parties is and shall remain independent parties. Neither Party nor any of their respective affiliates shall have the authority to enter into any contract or any obligation for, or make any warranty or representation on behalf of the other.

13.10 Expenses

Each of the Parties shall bear the fees and expenses of their respective counsels, accountants and experts and all other costs and expenses as may be incurred by them incidental to the negotiation, preparation, execution and delivery of this Agreement.

13.11 Surviving Provisions

13.11.1 The provisions of this Agreement, which are intended to survive the term of this Agreement by their very nature, shall survive the termination of this Agreement.

13.11.2 Notwithstanding the generality of the above, Clauses 8, 9 and 12 shall survive the termination/expiration of this Agreement.

13.12 Assignment

This Agreement shall not be assigned by either Party without obtaining a prior written consent from the other.

IN WITNESS WHEREOF the parties have each executed this Agreement by its duly authorized officer as of the day and year first above written.

SIGNED AND DELIVERED FOR AND ON BEHALF OF **THE PRESIDENT OF INDIA ACTING THROUGH (NAME & DESIGNATION) UNIQUE IDENTIFICATION AUTHORITY OF INDIA**

Title: _____

Designation: _____

Signature: _____

SIGNED AND DELIVERED FOR AND ON BEHALF OF

_____

Title: _____

Designation: _____

Signature: _____

WITNESSES:

Title: _____ Title: _____

Signature: _____ Signature: _____

SCHEDULE I
(Aadhaar Authentication Services – operation metrics and conditions)

1. The system designed by UIDAI for providing authentication services shall be available across multiple data centres. Other than planned outage the system is expected to run at 98% uptime which translates to about 3 hours of unexpected down time in a week.

2. The CIDR response time is expected to be between 1 to 3 seconds.

3. In order to ensure that the authentication service is friendly to the resident Aadhaar holder it is important that the authentication user agency and sub authentication user agency provide an efficient application to maintain end use latency under 5 seconds. AUAs/Sub-AUAs should consider round trip network latency from their devices to UIDAI data center and back while planning service roll out on the field. Depending on the choice of network and bandwidth, on the field performance may vary. It is important that for a good resident experience, AUAs/Sub-AUAs should try to keep the full round trip service time to be less than 8-10 seconds on an average.

4. In situations where OTP is being used as a factor for authentication, the delivery of the OTP to the Aadhaar number holder depends on SMS/Email delivery which is not in the control of UIDAI as these services are provided by external service providers. It is expected that OTP will be delivered within a reasonable time. AUAs/Sub-AUAs are encouraged to use OTP API to ensure reliability of inbound OTP request. OTP validity is specified within the message to make it easier and is currently kept at 30 min.

5. Authentication User Agency may be provided with various authentication tools and related services on demand for Authentication purposes. These tools would be augmented/improved/customized from time to time as per the requirement. AUA agencies would have to follow the entailing security and other operational requirements of such tools allowed for use and abide by any other instructions issued by UIDAI from time to time related thereof.

SCHEDULE- II

Purposes for which Aadhaar Authentication Services shall be used by the Authentication User Agency

ANNEXURE 1

e-KYC Agreement

(Annexure to UIDAI - AUA agreement)

1. Terms and Conditions

i. Aadhaar e-KYC is an Aadhaar Enabled Service offered by the UIDAI through the Authentication Service Agencies to Authentication User Agencies.

ii. Aadhaar e-KYC service is offered free of charge till a pricing policy decision is announced by UIDAI.

iii. UIDAI hereby grants the Authentication User Agency a non-exclusive and revocable right to use the Aadhaar e-KYC service to provide services to Aadhaar Holders. The Authentication User Agency understands that the Aadhaar e-KYC 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 e-KYC Service, at any time with prior notice, in its sole discretion, for any reason whatsoever. All the obligations of the Authentication User Agency under this agreement shall be equally applicable to the sub-AUAs.

iv. The Authentication User Agency hereby unequivocally agrees that all backend infrastructure, such as servers, databases etc., required specifically for the purpose of Aadhaar e-KYC shall be based in the territory of India.

v. It is hereby clearly understood by the Parties that UIDAI shall have no responsibility or liability in relation to failures that may take place during the Aadhaar e-KYC process.

2. Obligations of UIDAI

UIDAI shall:

i. Provide e-KYC data to the Authentication User Agency through the Authentication Service Agency upon authorization of the e-KYC request by an Aadhaar Holder, in the form of successful biometric or OTP-based Aadhaar authentication;

ii. Provide the e-KYC data in a manner conformant to the standards and processes described in the Demographic Data Standards and Verification Procedure (DDSVP) Committee Report;

iii. Provide e-KYC data conforming to Section 3 (Authentication of electronic Records), Section 4 (Legal recognition of electronic records), Section 5 (Legal recognition of digital signatures) and Section 6 (Use of electronic records and digital signatures in Government and its agencies) of the Information Technology Act, 2000;

iv. Determine and prescribe Standards and specifications for transmission of Aadhaar Identity Data for the purposes of Aadhaar e-KYC services;

v. Determine and prescribe standards to ensure the confidentiality, privacy and security of e-KYC data;

3. Obligations of Authentication User Agency

i. The Authentication User Agency shall maintain logs of all e-KYC transactions processed by it, capturing the complete details of the e-KYC transaction, such as the Aadhaar number against which e-KYC is sought, transaction code, authentication type, requesting AUA, requesting authentication device, date and timestamp, etc. as prescribed by UIDAI from time to time. The Authentication User Agency understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need-basis, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

ii. The e-KYC data resulting from an e-KYC request contains PID data for the purposes of service delivery. The storage of e-KYC data shall comply at all times with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

iii. The e-KYC data shall not be used by the AUA for purposes other than that for which the resident has explicitly given his/her consent.

iv. The AUA shall not share the e-KYC data with any other agency for purpose other than for the transaction as given in para (iii) above.

v. The AUA shall be responsible for obtaining the explicit consent (biometric or OTP based) of the resident for authorizing UIDAI to transfer his/her e-KYC details to the designated service provider.

vi. The AUA shall maintain records of obtaining the consent of the resident for a time period specified by UIDAI and allow access to UIDAI or any entity authorized by it to the related records.

सत्यमेव जयते

Aadhaar

Authentication Implementation Model

ASA – AUA Agreement Guidelines

Version 1.0

Unique Identification Authority of India

(UIDAI)

SUGGESTED GUIDELINES ON THE AGREEMENT BETWEEN ASA AND AUA

The following are the suggested guidelines on the clauses that the UIDAI recommends to be part of the agreement between the ASA and AUA. The AUA may include these clauses as part of its agreement with the ASA. The AUA and ASA may require sharing a copy of the signed agreement with UIDAI, as and when requested by UIDAI.

1. ASAs are empanelled by UIDAI to provide UIDAI-compliant secured network connectivity as a service to Authentication User Agencies and transmit AUAs' authentication requests to CIDR.

2. ASA shall not provide any secured network connectivity between the CIDR and the AUA or its Sub AUA immediately upon receipt of notification from UIDAI of termination of contract between UIDAI and the AUA or its Sub AUAs.

3. AUA or its Sub AUAs shall not deal with such ASAs for connectivity to the CIDR immediately upon receipt of notification from UIDAI of termination of contract between UIDAI and the ASA.

4. ASA shall forward to CIDR only requests that are complete and incomplete authentication requests shall be returned with appropriate error message.

5. AUA is an AUA as long as it is designated as an AUA by the UIDAI and the day it ceases to be an AUA, all the contracts between the ASA and AUA will stand terminated without any notice

6. AUA shall take due care to provide only complete and compliant request for authentication to ASA.

7. The AUA shall ensure that the network connectivity used for sending their authentication requests is in compliance with UIDAI's standards and specifications. The AUA shall build and maintain the connectivity between authentication devices and the ASA's systems by themselves or through an outsourced service provider.

8. The AUA shall ensure that the authentication devices used for enabling Aadhaar authentication for its services shall comply with UIDAI's specifications and standards; and that the applications driving the authentication devices are certified by UIDAI (or UIDAI-approved independent certification agency).

9. The Authentication User Agency unequivocally agrees that all applications used by it in running its Aadhaar authentication operations shall be duly certified/ approved by UIDAI or an agency appointed/ approved by UIDAI (as and when UIDAI creates a certification mechanism for certifying Aadhaar enabled applications). In the event the already certified/ approved applications employed by the Authentication User Agency undergo modifications, the Authentication User Agency shall deploy the modified applications only after renewed certification/ approval from UIDAI.

10. Both ASA and AUA shall ensure that all relevant laws and regulations are adhered to in relation to data storage and data protection (with regard to Aadhaar-based identity data) in their systems, that of their agents (if applicable) and with authentication devices.

11. In cases where the authentication devices are operated by AUA's personnel (or personnel of their agents), the AUA is responsible for ensuring that the operating personnel who are adequately trained to conduct Aadhaar-based authentication in compliance with UIDAI's requirements.

12. When an AUA engages with a Sub AUA, it generates a Sub AUA Code to identify the specific Sub AUA. When transmitting authentication requests from a Sub AUA, the AUA always includes the Sub AUA Code so that Aadhaar authentication transaction logs can track the origin of all authentication requests.

13. The AUA shall take responsibility on behalf of their Sub AUAs for the standards to be maintained regarding security, infrastructure, processes, devices and other aspects as specified by UIDAI The AUAs shall take responsibility on behalf of their Sub AUAs for completeness of the authentication requests.

14. AUAs shall inform ASAs of any termination of contracts with Sub AUAs

सत्यमेव जयते

Aadhaar

Authentication Implementation Model

AUA – Sub AUA Agreement Guidelines

Version 1.0

AADHAAR

Unique Identification Authority of India

(UIDAI)

SUGGESTED GUIDELINES ON THE AGREEMENT BETWEEN AUA AND Sub AUA

These are some suggested clauses which may be included in the agreement between an AUA and Sub AUA

1. The Sub AUA who is seeking to use Aadhaar Authentication to enable a specific service/business function is solely responsible for the choice of authentication type(s). The choice of the Authentication type shall be the sole decision of the Sub AUA, and no other entity, including UIDAI, Authentication Service Agency and Aadhaar Holder shall have any role in this decision of Sub AUA.

2. The Sub AUA assumes complete responsibility with regard to its network connectivity with an Authentication User Agency and UIDAI shall have no responsibility in this regard.

3. The Sub AUA shall establish and maintain necessary authentication related operations, including systems, processes, infrastructure, technology, security, etc., which may be necessary for using Aadhaar Authentication Service, in compliance with standards and specifications, issued by UIDAI from time to time.

4. The Authentication User Agency and the Sub AUA shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners) which are duly registered with/ approved/ certified by UIDAI or an agency appointed by UIDAI for this purpose. Both parties understand the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which confirm to the authentication type adopted by the Sub AUA, and UIDAI shall have no role to play in this regard, and shall have no liability or responsibility in this respect.

5. The Sub AUA shall ensure that the persons employed by it for providing Aadhaar Enabled Services and for maintaining necessary systems, infrastructure, processes, etc. in this regard, possess requisite qualifications for undertaking such works. The Sub AUA shall be responsible for ensuring that such personnel are suitably and adequately trained to conduct Aadhaar Enabled Services, in compliance with specifications and standards prescribed by UIDAI from time to time.

6. The Sub AUA shall, at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed there under, from time to time, in so far as the same has application to its operations in accordance with this Agreement, and also with all other Laws, rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security and management, data storage, sharing and data protection, as also with the National Identification Authority of India Bill, as and when the same in enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device.

7. The Sub AUAs shall maintain logs of all authentication transactions processed by it, capturing the complete details of the authentication transaction and shall retain the same for a duration as prescribed by UIDAI from time to time but shall not, in any event, store the Aadhaar Personal Identity Data of the Aadhaar Holder. (PID) . The Sub AUA understands and agrees that the logs maintained by it shall not be shared with any individual or entity, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

8. In case of any investigations around authentication related fraud(s) or dispute (s), the Sub AUA shall extend full cooperation to UIDAI, and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource / information, etc. of or pertaining to its Authentication Device.

9. The Sub AUA unequivocally agrees that all applications used by it in running its Aadhaar authentication operations shall be duly certified/ approved by UIDAI or an agency appointed/ approved by UIDAI (as and when UIDAI creates a certification mechanism for certifying Aadhaar enabled applications),. In the event the already certified/ approved applications employed by the Sub AUA undergo modifications, the Sub AUA shall deploy the modified applications only after renewed certification/ approval from UIDAI.

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

AADHAAR OTP REQUEST API

API SPECIFICATION - VERSION 1.6

APRIL 2015

Table of Contents

1. INTRODUCTION 3
1.1 AUTHENTICATION FACTORS AND ONE TIME PIN (OTP) 3
1.2 TARGET AUDIENCE AND PRE-REQUISITES 4
1.3 OBJECTIVE OF THIS DOCUMENT 4
2. OTP REQUEST API 5
2.1 OTP USAGE SCENARIO 5
2.2 OTP REQUEST PROCESS 5
2.3 API PROTOCOL 6
2.3.1 *Element Details* *6*
2.4 API REQUEST DATA FORMAT 7
2.4.1 *Element Details* *7*
2.5 API RESPONSE DATA FORMAT 10
2.5.1 *Element Details* *10*

1. Introduction

The Unique Identification Authority of India (UIDAI) has been created, with the mandate of providing a Unique Identity (Aadhaar) to all Indian residents. The UIDAI proposes to provide online authentication using demographic and biometric data.

Aadhaar "*authentication*" means the process wherein Aadhaar Number, along with other attributes, including biometrics, are submitted to the Central Identities Data Repository (CIDR) for its verification on the basis of information or data or documents available with it. UIDAI will provide an online service to support this process. Aadhaar authentication service only responds with a "yes/no" and no personal identity information is returned as part of the response.

1.1 Authentication Factors and One Time Pin (OTP)

Authentication focuses on matching a person's identity based on the reliability of a credential offered. Various agencies have different requirements for the degree of assurance required while authenticating beneficiaries/customers. When authenticating a resident, multiple factors may be used to strengthen the authenticity of the request.

In general, following are the 3 categories of factors:

1. ***What you have***: Something the user uniquely has (e.g., a card, security token, mobile phone, access to email account, etc.)
2. ***What you know***: Something the user knows that is not public (e.g., a password, PIN, secret question, etc.). Demographic details such as date of birth may also be classified in this category although they are generally considered weak factors.
3. ***Who you are***: Something the user individually is or does (e.g., fingerprint pattern, iris pattern, signature, handwriting, etc.).

Aadhaar authentication provides multi-factor authentication to AUAs based on the following factors:

1. *What you have* – Mobile phone, email account
2. *What you know* –PIN, used ONLY for internal UIDAI transactions
3. *Who you are* – Fingerprints and Iris

When user agencies (AUAs) adopt Aadhaar authentication, they can choose option 1 or 3 above or both. Resident authentication can be strengthened by using multi-factor authentication.

To obtain OTP, following two ways can be used:

- By the resident her/himself using resident portal, by sending an inbound SMS from registered phone, by calling IVR from registered phone, or by using UIDAI provided mobile app running on registered phone.

- By programmatically initiating the request from the AUA/sub-AUA application in which authentication is used. Whichever application needing to validate OTP can thus initiate OTP request on behalf of the resident via an API. This document covers this API details for "***Application Initiated***" OTP request.

Notice that OTP is always delivered on the resident's mobile/email and application is expected to capture that OTP from the resident and pass it within the authentication request to authenticate the Aadhaar holder.

1.2 Target Audience and Pre-Requisites

This is a technical document and is targeted at software professionals working in technology domain and interested in incorporating Aadhaar authentication into their applications.

Readers must be fully familiar with following authentication documents published on UIDAI website (http://uidai.gov.in/auth) before reading this document.

1. Aadhaar Authentication Framework - http://uidai.gov.in/images/authDoc/d2_authentication_framework_v1.pdf
2. Aadhaar Authentication Operating Model - http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf
3. Aadhaar Authentication API Specifications - http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf

1.3 Objective of this document

This document provides Aadhaar OTP Request API specification for applications to request OTP on behalf of the resident. It contains details including API data format, protocol, and security specifications.

2. OTP Request API

This chapter describes the AUA/Sub-AUA application initiated OTP request API in detail including the flow, communication protocol, and data formats.

2.1 OTP Usage Scenario

Aadhaar authentication supports biometrics and/or One Time Pin (OTP) based authentication. While biometrics provide one factor (who you are), OTP provide another factor (what you have). Applications that take advantage of Aadhaar Authentication can use OTP to provide single factor authentication or along with biometrics for achieving two factor authentication.

When using OTP, at a high level, there are two distinct activities:

1. Resident obtaining the OTP on her/his phone/email. As described earlier, resident can obtain this directly from UIDAI servers via mobile app, inbound SMS, etc., or application can request an OTP to be sent to resident via this API.
    a. Applications should ask resident to enter OTP if the resident already has an OTP.
    b. If the resident does not have one, applications can initiate on behalf of the resident via this API.
2. Application requests the resident to provide the OTP. This OTP value should then be used within the Authentication API request by adding "Pv" element into the PID block (see Authentication API 1.6 Specification for details).

It's important to understand that the above two steps are two disconnected API calls and OTP value generated from using the OTP API (step 1 above) is then used as part of Authentication API to actually validate OTP via authentication (step 2 above).

Since OTP usage assumes that the resident is aware of the transaction (to be able to provide the OTP value received on his/her mobile/email to application), only a maximum of one OTP is valid for an Aadhaar number at any point in time. Every time a new OTP is generated, previous OTP, if any, cease to be valid. OTP generated has an expiry period for security reasons and it is expected that resident uses the OTP within that time. If not used, a new OTP needs to be generated for next transaction.

2.2 OTP Request Process

Application initiated OTP request works as follows:

1. Application (an application on an assisted device or self-service kiosks, or applications on the Internet), wanting to use Aadhaar OTP as a factor within Aadhaar authentication, initiates the transaction flow.
2. Application captures Aadhaar number along with any other data as needed.

3. Application, through AUA server, invokes the OTP Request API by forming digitally signed API Input XML (format explained later in this document).
4. UIDAI server processes the input, validates it, generates OTP, and sends it to resident's registered mobile/email.
5. UIDAI server then responds to OTP Request API with a response XML with success or indicating any error (see response XML details in later sections).
6. Resident receives the OTP from Aadhaar server on his/her email and/or mobile.
7. Application then requests resident to provide the OTP value so that application can send that via Aadhaar authentication API for authenticating the resident.

After receiving OTP, subsequent usage of OTP within Aadhaar authentication is explained in Aadhaar Authentication API specification 1.6. Notice that OTP expires with a UIDAI stipulated time. OTP message (SMS/Email) sent to resident provides time at which OTP was generated and when it is going to expire.

Applications should not initiate OTP request without the resident having to explicitly request the service offered by the agency and also should make sure that resident is made aware of OTP usage so that no OTP is sent to resident without his/her knowledge.

2.3 API Protocol

Aadhaar OTP Request API is exposed as stateless service over HTTPS. Usage of open data format in XML and widely used protocol such as HTTP allows easy adoption and deployment of these services.

Following is the URL format for Aadhaar OTP service:

```
https://<host>/otp/<ver>/<ac>/<uid[0]>/<uid[1]>/<asalk>
```

API input data should be sent to this URL as XML document using Content-Type "application/xml" or "text/xml".

As a best practice, for all SSL communications the agencies should automatically validate the SSL certificate and ensure it is validated against the revocation list online.

2.3.1 Element Details

host – Aadhaar OTP server address. Actual production server address will be provided to ASAs. Note that production servers can only be accessed through secure links. For development and testing purposes, public URL "*auth.uidai.gov.in*" can be used. ASA server should ensure that actual URL is configurable for flexibility.

Next part of the URL "otp" indicates that this is a OTP Request API call instead of regular authentication API call. Ensure that this is provided.

ver – OTP API version (mandatory). If not provided, URL points to current version. UIDAI may host multiple versions for supporting gradual migration. Version of this API is "1.6".

ac – A unique code for the AUA which is assigned by UIDAI. This is an alpha-numeric string having maximum length 10. (A default value "public" is available for testing.)

uid[0] and **uid[1]** – First 2 digits of Aadhaar Number of the resident for whom the OTP is being requested for. This is used for internal load-balancing.

asalk – A valid ASA license key. ASAs must send one of their valid license keys at the end of the URL. It is important that license keys are maintained safely. When adding license key to the URL, ensure it is "URL encoded" to handle special characters.

For all valid responses, HTTP response code 200 is used. All application error codes are encapsulated in response XML element. In the case of connection and other server errors, standard HTTP error response codes are used (4xx codes such as 403, 404, etc.). HTTP automatic redirects also should be handled by ASA server.

2.4 API Request Data Format

Aadhaar OTP service uses XML as the data format for input and output. To avoid sending unnecessary data, do not pass any optional attribute or element unless its value is different from default value. Any bad data or extra data will be rejected.

Following is the XML data format for OTP API:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Otp uid="" tid="" ac="" sa="" ver="" txn="" lk="" type="">
  <Opts ch=""/>
  <Signature>Digital signature of AUA</Signature>
</Otp>
```

2.4.1 Element Details

Element: **Otp** (mandatory)

- Root element of the input XML for OTP service.

Attributes:

- **uid** – (mandatory) – If requesting for an OTP against an Aadhaar number for authentication, provide 12 digit Aadhaar number in this field. But, if this API is used for obtaining a verification code for a mobile (e.g., for mobile update API), provide 10 digit mobile number (excluding country code, it is assumed to be

India for now). If mobile number is given instead of Aadhaar number in this field "type" attribute MUST BE set to "M".

- **tid** – (mandatory) For Registered devices, send its unique Terminal ID. For Public devices, value should be passed as "public".
- **ac** – (mandatory) A unique code for the AUA which is assigned by UIDAI during AUA registration process. This is an alpha-numeric string having maximum length 10. (A Default value "public" is available only for testing.)
- **sa** – (mandatory) A unique "Sub-AUA" code. AUAs are expected to manage these codes within their system and ensure uniqueness within their system. This allows auditing and business intelligence to be provided at SA level. If AUA and SA are same agency, use value of "ac" for this attribute. This is an alpha-numeric string having maximum length 10.
- **ver** – (mandatory) version of the OTP API. Currently only valid value is "1.6".
- **txn** – (mandatory) AUA specific transaction identifier. AUA can choose to pass this as part of input. This is returned as part of response as is. This is very useful for linking transactions full round trip across systems. This is an alpha-numeric string of maximum length 50. Only supported characters are A-Z, a-z, 0-9, period, comma, hyphen, backward & forward slash, left & right parenthesis, and colon. No other characters are supported. It is highly recommended that AUAs use this attribute for correlating requests with responses for auditing and verification.
- **lk** – (mandatory) A valid "License Key" assigned to the AUA. Administration portal of UIDAI will provide a mechanism for AUA administrator to generate license keys. This is an alpha-numeric string of length up to 64 characters.
- **type** – (optional) Type of OTP request. Possible values are:
    - "A" – uid attribute value shall refer to Aadhaar number (this is the default option). If this attribute is missing, it is assumed that "uid" field contains a valid Aadhaar number.
    - "M" – uid attribute value shall refer to new mobile number (this is used when a verification code needs to be sent to a mobile number, see mobile update API for details).

  Note: You can use any valid license key that has OTP feature enabled for this purpose.

Element: **Opts** (Optional)

- Various options are provided under this element.

Attributes:

- **ch** – (Optional) Valid only when using OTP against an Aadhaar number (when using Aadhaar number in "uid" attribute). Channel through which OTP should be sent. Possible values are:
    - "00" – send OTP via both SMS and Email (this is the default)
    - "01" – send OTP via SMS only
    - "02" – send OTP via Email only

  If type attribute is set to "M", notification shall be sent ONLY to the given mobile number via SMS. Any value in this "ch" attribute will be ignored.

Element: **Signature** (mandatory)

- The request XML should be digitally signed for message integrity and non-repudiation purposes.
- Digital signing should always be performed by the entity that creates the final request XML
    1. AUA can digitally sign after forming the API input XML. This is almost always the case. In such cases, AUA ensures the message security and integrity between AUA servers and its client applications.
    2. ASA can digitally sign the request XML if it is a domain-specific aggregator and forms the request XML on behalf of the AUA. In such cases, ASA and AUA ensure the message security and integrity between their servers.
- Procuring digital signature certificates:
    1. It should be procured from a valid certification authority as per Indian IT Act (see http://cca.gov.in/rw/pages/faqs.en.do#thecaslicensedbythecca)
    2. Digital certificates have two parts:
        - X.509 certificate representing public key.
        - Private Key which is used for digital signing. Private Key should be stored securely and is the responsibility of the owner of the certificate to ensure that it is not compromised.
    3. It should be a class II or class III certificate.
    4. X.509 certificate contains information about the owner of the certificate; in this case it will be details of the person and the organization to which he/she belongs. UIDAI server checks to ensure that certificate belongs to the ASA or AUA organization. Hence, it is mandatory that "O" attribute of "Subject" in the X.509 certificate matches the name of the organization.
- Digital signing of request XML
    1. XML digital signature algorithm as recommended by W3C.
    2. Signature should include key info element that contains X.509 certificate details. This is needed for UIDAI server to validate the signer.
- Verification of digital signature by UIDAI servers. UIDAI server validates the signature in the following sequence:
    1. Checks if the signature element is present. If not, it throws an error.
    2. If signature element is present, then it validates if the certificate is issued by one of the valid certification authority. If not valid, throws error.
    3. If it is a valid certificate, then it validates whether the "O" attribute in the X.509 certificate's subject matches the AUA organization name. If yes, proceeds with API logic.
    4. If it does not match AUA organization name, it checks configuration to see if ASA is allowed to sign on behalf of that AUA. If not, throws error.
    5. If ASA is allowed to sign on behalf of that AUA, it checks whether the "O" element of the certificate matches with the organization name of the ASA. If not, throws error.
    6. If it matches, it proceeds with API logic.
    7. In either case, once it is determined that request XML has been signed by either the AUA or ASA and is issued by a valid CA, UIDAI server will then check whether the certificate is white listed by AUA or ASA in the UIDAI Web portal.

- UIDAI web portal will optionally allow ASA and AUA users to upload public certificates used for signing.
- This provides for an option wherein ASA or AUA can choose to delete a certificate from the UIDAI portal in case it gets expired or is compromised. This acts as an additional security check.

2.5 API Response Data Format

Response XML is as follows:

```
<OtpRes ret="" code="" txn="" err="" ts="" info=""/>
```

2.5.1 Element Details

Element: **OtpRes**

Attributes:

- **ret** – Result of OTP generation request. "y" if successful, "n" if failure in which case "err" attribute will provide the reason of failure.
- **code** – Unique alphanumeric "OTP response" code having maximum length 40.
- **txn** – AUA specific transaction identifier. This is exactly the same value that is sent within the request.
- **ts** – Timestamp when the response is generated. This is of type XSD dateTime.
- **err** – Failure error code. If OTP request fails, this attribute provides any of the following codes (for updates, see https://developer.uidai.gov.in/site/api_err):
  - "**110**" – Aadhaar number does not have verified mobile/email
  - "**111**" – Aadhaar number does not have verified mobile
  - "**112**" – Aadhaar number does not have both email and mobile.
  - **"510"** – Invalid "Otp" XML format
  - **"520"** – Invalid device
  - **"521"** – Invalid mobile number
  - **"522"** – Invalid "type" attribute
  - **"530"** – Invalid AUA code
  - **"540"** – Invalid OTP XML version
  - **"542"** – AUA not authorized for ASA. This error will be returned if AUA and ASA do not have linking in the portal
  - **"543"** – Sub-AUA not associated with "AUA". This error will be returned if Sub-AUA specified in "sa" attribute is not added as "Sub-AUA" in portal
  - **"565" –** AUA License key has expired or is invalid
  - **"566" –** ASA license key has expired or is invalid
  - **"569"** – Digital signature verification failed
  - **"570"** – Invalid key info in digital signature (this means that certificate used for signing the OTP request is not valid – it is either expired, or does not belong to the AUA or is not created by a CA)
  - **"940"** – Unauthorized ASA channel
  - **"941"** – Unspecified ASA channel
  - **"950"** – Could not generate and/or send OTP
  - **"999"** – Unknown error

- **info** – Info block having masked mobile number and/or email to help application show appropriate message to resident. Length of "info" can be up to 256 characters and is composed of the following parts. Format of the info block is:
  <Version>{SHA-256 of Aadhaar Number, timestamp, OTP_api_ver, SHA-256 of ASA code, SHA-256 of AUA code, Sub-AUA code, masked-mobile, masked-email}
  - "Version" – is the version of the info structure. Currently "01"
  - "SHA-256 of Aadhaar Number" – is the SHA-256 hash value of Aadhaar Number provided as part of input
  - "SHA-256 of ASA code" – is the SHA-256 hash value of AUA code provided as part of input.
  - "SHA-256 of AUA code" – is the SHA-256 hash value of ASA code provided as part of input.
  - "Sub-AUA code" – same as the sub-AUA code passed in request.
  - "OTP_api_ver" – version of OTP Request API
  - "timestamp" – timestamp of the request.
  - "masked-mobile" – Masked mobile number. If this is not empty, AUA/Sub-AUA application can use this to display message "*OTP has been sent to mobile number <masked-mobile>"*
  - "masked-email" – Masked email id. If this is not empty, AUA/Sub-AUA application can use this to display message "*OTP has been sent to email ID <masked-email>"*

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

AADHAAR AUTHENTICATION

API SPECIFICATION - VERSION 2.0

MAY 2016

Table of Contents

1. INTRODUCTION 3
   - 1.1 Target Audience and Pre-Requisites 3
   - 1.2 Terminology 4
   - 1.3 Legal Framework 5
   - 1.4 Objective of this document 5
2. UNDERSTANDING AADHAAR AUTHENTICATION 6
   - 2.1 Aadhaar Number 6
   - 2.2 Aadhaar Authentication at a Glance 6
   - 2.3 Aadhaar Authentication Usage 7
   - 2.4 Conclusion 7
3. AADHAAR AUTHENTICATION API 8
   - 3.1 Authentication Flow 8
   - 3.2 API Protocol 9
     - *3.2.1 Element Details 10*
   - 3.3 Authentication API: Input Data Format 11
     - *3.3.1 Element Details 12*
   - 3.4 Authentication API: Response Data Format 24
     - *3.4.1 Element Details 25*
4. API AND DATA SECURITY 32
   - 4.1 Authentication Data Security 32
   - 4.2 Using Registered Devices 33
   - 4.3 Using Synchronized Session Key 33
   - 4.4 Using Binary format for PID block 33
   - 4.5 Authentication Audits 34
5. APPENDIX 35
   - 5.1 Related Publications 35
   - 5.2 Changes in Version 2.0 from Version 1.6 36

1. Introduction

The Unique Identification Authority of India (UIDAI) has been created, with the mandate of providing a Unique Identity (Aadhaar) to all Indian residents. The UIDAI provides online authentication to verify the identity claim of the Aadhaar holder.

Aadhaar "*authentication*" means the process wherein Aadhaar Number, along with other attributes, including biometrics, are submitted to the Central Identities Data Repository (CIDR) for its verification on the basis of information or data or documents available with it. UIDAI provides an online service to support this process. Aadhaar authentication service only responds with a "yes/no" and no personal identity information is returned as part of the response.

1.1 Target Audience and Pre-Requisites

This is a technical document and is targeted at software professionals working in technology domain and interested in incorporating Aadhaar authentication into their applications.

Before reading this document, readers are highly encouraged to read the following documents to understand the overall system:

1. UIDAI Strategy Overview - http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overview-001.pdf
2. The Demographic Data Standards and verification procedure Committee Report - http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
3. The Biometrics Standards Committee Report - http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf
4. From Exclusion to Inclusion with Micropayments - http://uidai.gov.in/images/FrontPageUpdates/microatmstandardsv1.3.pdf
5. Aadhaar-Communicating to a billion : An Awareness and Communication Report - http://uidai.gov.in/UID_PDF/Front_Page_Articles/Events/AADHAAR_PDF.pdf

Readers must also read the following related documents for complete understanding.

1. Aadhaar Best Finger Detection API - http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf
2. Aadhaar OTP Request API - http://uidai.gov.in/images/resource/aadhaar_otp_request_api_1_6.pdf
3. Aadhaar Registered Devices Specification - http://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0.pdf

1.2 Terminology

Authentication User Agency (AUA): An organization or an entity using Aadhaar authentication as part of its applications to provide services to residents. Examples include Government Departments, Banks, and other public or private organizations. All AUAs (Authentication User Agencies) must be registered within Aadhaar authentication server to perform secure authentication.

Sub-AUA (SA): An organization or a department or an entity having a business relationship with AUA offering specific services in a particular domain. All authentication requests emerging from an AUA contains the information on the specific SA. For example, a specific bank providing Aadhaar enabled payment transaction through NPCI as the AUA becomes the SA. Similarly, a state government being an AUA can have the health department under them as the SA using Aadhaar authentication while providing healthcare benefits.

Authentication Service Agency (ASA): An organization or an entity providing secure leased line connectivity to UIDAI's data centres for transmitting authentication requests from various AUAs. All connections to production authentication servers must come through private and secure connection through ASAs. Those AUAs who wish to provide their connectivity can become their own ASA whereas smaller AUAs who do not wish to create direct leased line connection to UIDAI's data centres can use an ASA.

Terminal/Host Devices: Terminal/Host devices are devices employed by SAs/AUAs (both government and non-government) to provide services to the residents. Examples include MicroATM devices, PoS devices, PDS terminals, Smart phones, laptops, tablets, access control systems, etc. These devices will host the applications of the SA/AUA and support biometric capture mechanism to capture biometrics of residents for authentication purposes. Any additional features of these terminal devices would depend on specific needs of services offered by SAs/AUAs. Applications that uses Aadhaar Authentication on these devices must comply with specifications issues by UIDAI to protect all the biometric and demographic information provided by the residents.

Registered and Public Devices: Term "Registered Devices" refers to devices which are capable to manage public digital certificate keys. Aadhaar authentication server can individually identify and validate these devices to ensure biometrics are captured by them. Term "Public Devices" refers to devices which are not registered with Aadhaar system and uses its own encryption key generation scheme. Aadhaar authentication server does not individually identify public devices and uses an alternate encryption strategy for them.

Authentication Factors: Aadhaar authentication supports authentication using multiple factors. These factors include demographic data, biometric data, PIN, OTP, possession of mobile, or combinations thereof. Adding multiple factors increases the strength of authentication depending on the factors. Applications using Aadhaar authentication need

to choose appropriate authentication factors based on the application needs. Currently, not all factors are supported.

Matching Strategy: Various demographic and biometric matchers use fuzzy matching and work on match thresholds and not on absolute digital (0 or 1) outputs, the interpretation of match scores to a MATCH or NON-MATCH needs to be tuneable using matching strategy. For demographic data matching, currently "Exact" and "Partial" matching strategies are supported in English and fuzzy matching of Indian language data is also supported.

1.3 Legal Framework

UIDAI has developed necessary legal framework and processes around Aadhaar authentication. These documents specify AUA/ASA registration process, security framework, operating model and covers their obligations, responsibilities and liabilities.

1.4 Objective of this document

This document provides Aadhaar Authentication API (Application Programming Interface) specification. It contains details including API data format, protocol, and security specifications.

For latest documents related to Aadhaar authentication and other Aadhaar APIs, see http://authportal.uidai.gov.in

2. Understanding Aadhaar Authentication

This chapter describes Aadhaar authentication, some of the envisioned usage scenarios, and working details. Technical details follow in subsequent chapters.

2.1 Aadhaar Number

The Unique Identification (Aadhaar) Number, which identifies a resident, gives individuals the means to clearly establish their identity to public and private agencies across the country. Three key characteristics of Aadhaar Number are:

1. Permanency (Aadhaar number remains same during lifetime of a resident)
2. Uniqueness (one resident has one ID and no two residents have same ID)
3. Global (same identifier can be used across applications and domains)

Aadhaar Number is provided during the initiation process called *enrolment* where a resident's demographic and biometric information are collected and uniqueness of the provided data is established through a process called *de-duplication*. Post de-duplication, an Aadhaar Number is issued and a letter is sent to resident informing the details.

2.2 Aadhaar Authentication at a Glance

Aadhaar authentication is the process wherein Aadhaar Number, along with other attributes, including biometrics, are submitted online to the CIDR for its verification on the basis of information or data or documents available with it.

In all forms of authentication the Aadhaar Number needs to be submitted so that authentication is reduced to a 1:1 match. In addition, Aadhaar authentication service only responds with a "yes/no" and no Personal Identity Information (PII) is returned as part of the response.

Aadhaar authentication provides several ways in which a resident can authenticate themselves using the system. At a high level, authentication can be using Demographics data and/or Biometric (FP/Iris/Face) data, and/or OTP. **Face authentication is currently not supported**.

During the authentication transaction, the resident's record is first selected using the Aadhaar Number and then the demographic/biometric inputs are matched against the stored data within CIDR which was provided by the resident during enrolment/update process.

2.3 Aadhaar Authentication Usage

Aadhaar authentication enables agencies to verify identity of residents using an online and electronic means where the agency collects required information from the resident along with resident's Aadhaar Number and passes the same to UIDAI systems for verification.

Aadhaar authentication service provides services to instantly verify the identity of the resident against the available data in CIDR. Based on the needs of the service, different identifiers could be used along with Aadhaar Number. These identifiers could be combination of biometrics (such as fingerprints, iris impressions) and/or demographic information (such as Name, Date of birth, Address) and/or a secret PIN or OTP number known only to the resident.

Aadhaar Number along with certain demographic information such as name of the resident, date of birth, etc. helps to provides for simple authentication needs. For example, when MGNREGA beneficiary is enrolled and given a job card, resident could be biometrically authenticated against Aadhaar system to verify his/her Aadhaar number along with name, address.

Combination of Aadhaar Number and biometrics deliver online authentication without needing a card. During biometric authentication, agency will collect the Aadhaar Number along with one or more biometric impressions (e.g., one or more fingerprints, or iris impression alone or iris impression along with fingerprints). The information collected could then be passed to Aadhaar authentication server for authenticating the resident. In addition, AUA specific factors such as cards may also be used in conjunction with Aadhaar authentication.

For further details on usage of Aadhaar in various service delivery scenarios, refer to "Aadhaar Enabled Service Delivery" White Paper published on UIDAI website - http://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf

2.4 Conclusion

Aadhaar authentication provides a convenient mechanism for all residents to establish their identity. It provides a national platform for identity authentication and can be used to deliver services effectively to residents across the country.

Rest of the document is technical in nature and is intended for software professionals working with applications wanting to enable their applications to support Aadhaar authentication.

3. Aadhaar Authentication API

This chapter describes the API in detail including the authentication flow, communication protocol, and data formats.

3.1 Authentication Flow

Following diagram explains various authentication scenarios and data flow.

Scenario (1) in the diagram is a typical authentication flow and is a case of an operator assisted transaction at a PoS terminal:

a) Resident provides Aadhaar Number, necessary demographic and biometric details to terminal devices belonging to the AUA/SA (or merchant/operator appointed by AUA/SA) to obtain a service offered by the AUA/SA.
b) Aadhaar authentication enabled application software that is installed on the device packages these input parameters, encrypts, and sends it to AUA server over either a mobile/broadband network using AUA specific protocol.
c) AUA server, after validation, adds necessary headers (AUA specific wrapper XML with license key, transaction id, etc.), and passes the request through ASA server to UIDAI CIDR.
d) Aadhaar authentication server returns a "yes/no" based on the match of the input parameters.
e) Based on the response from the Aadhaar authentication server, AUA/SA conducts the transaction.

Scenario (2) below depicts the resident conducting assisted/self-service transactions with Aadhaar authentication on his/her mobile or on the Internet.

a) In this case, transaction data is captured on the mobile/Internet application provided by AUA/SA to residents
b) Resident provides necessary demographic data long with OTP (fingerprint/iris is also possible although not yet common on mobiles or PCs) in addition to AUA specific attributes (account number, password, PIN, etc.)
c) Step c, d, and e are same as in scenario 1 above.

Scenario (3) is a slight variant of 2nd scenario where AUA also plays the role of ASA and has direct connectivity to UIDAI data centers. Scenario (4) is how AUAs and application developers can test Aadhaar authentication using the public URL.

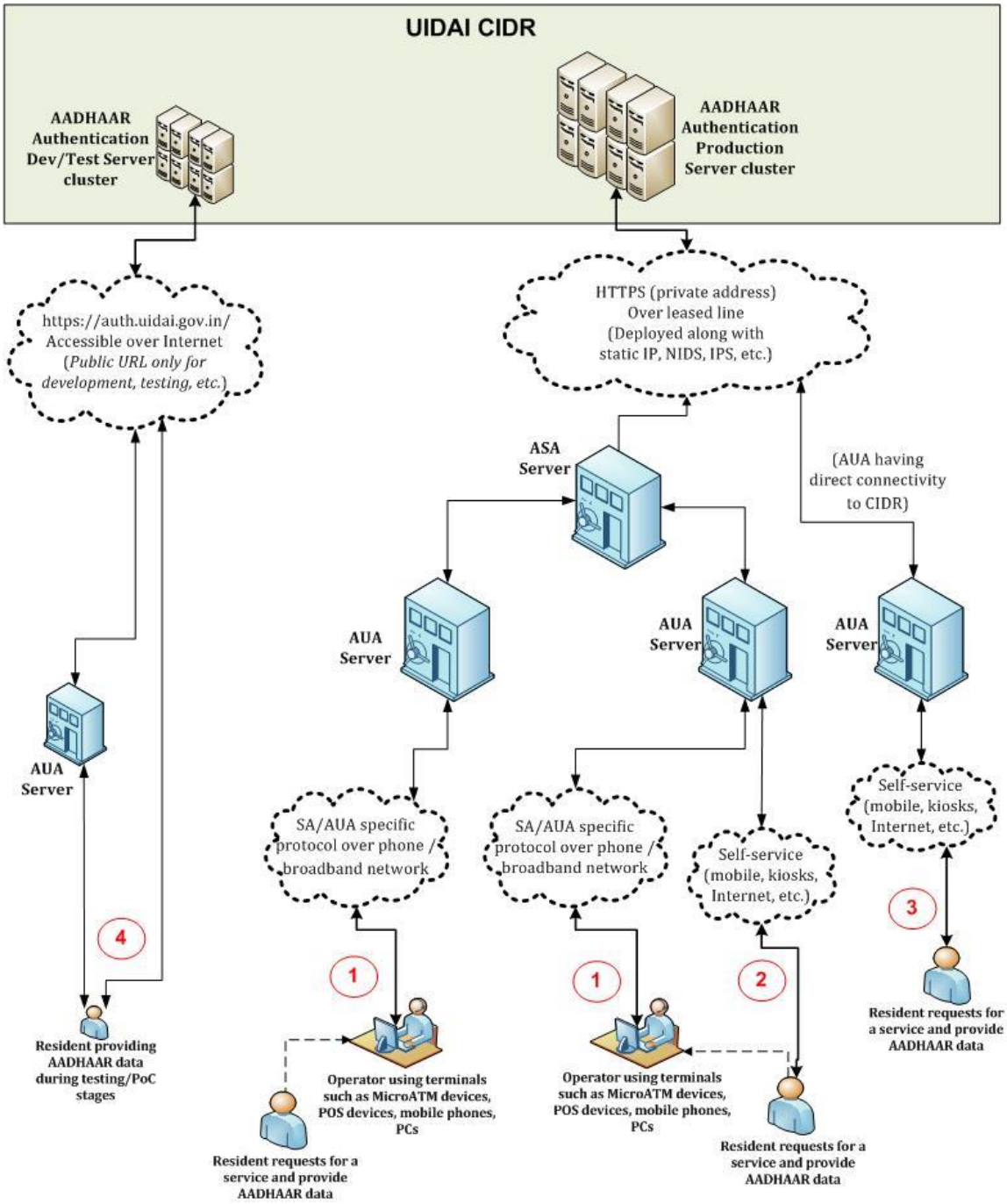


Figure 1: Aadhaar authentication flow under various scenarios

3.2 API Protocol

Aadhaar authentication service is exposed as stateless service over HTTPS. Usage of open data format in XML and widely used protocol such as HTTP allows easy adoption and deployment of Aadhaar authentication. To support strong end to end security and avoid request tampering and man-in-the-middle attacks, it is essential that encryption of data happens at the time of capture on the capture device.

Following is the URL format for Aadhaar authentication service:

```
https://<host>/<ver>/<ac>/<uid[0]>/<uid[1]>/<asalk>
```

API input data should be sent to this URL as XML document using Content-Type "application/xml" or "text/xml".

For security reason data collected for Aadhaar authentication must not be stored in the devices or log files. It's essential for ASA and AUA to maintain audit records for all the authentication request metadata along with the response.

As a best practice, for all secure communications the agencies should automatically validate the SSL/TLS certificate and ensure it is validated against the revocation list online.

3.2.1 Element Details

host – Aadhaar authentication server address. Actual production server address will be provided to ASAs. Note that production servers can only be accessed through private secure connection. ASA server should ensure that actual URL is configurable. (*For development and testing purposes, public URL "auth.uidai.gov.in" can be used.*)

ver – Authentication API version (optional). If not provided, URL points to current version. UIDAI may host multiple versions for supporting gradual migration. As of this specification, default production version is "**2.0**".

ac – A unique code for the AUA which is assigned by UIDAI. This is an alpha-numeric string having maximum length 10. (A default value "public" is available for testing.)

uid[0] and **uid[1]** – First 2 digits of Aadhaar Number. Used for load-balancing.

asalk – A valid ASA license key. ASAs must send one of their valid license keys at the end of the URL. It is important that license keys are maintained safely. **When adding license key to the URL, ensure it is "URL encoded" to handle special characters**.

For all valid responses, HTTP response code 200 is used. All application error codes are encapsulated in response XML element. In the case of connection and other server errors, standard HTTP error response codes are used (4xx codes such as 403, 404, etc.). HTTP automatic redirects also should be handled by ASA server.

ASA server must send one of their valid license keys as part of the URL (see details above). Authentication related APIs are enabled only for valid ASAs and only for their registered static IP addresses coming through a secure private network.

3.3 Authentication API: Input Data Format

Aadhaar authentication uses XML as the data format for input and output. To avoid sending unnecessary data, do not pass any optional attribute or element unless its value is different from default value. Any bad data or extra data will be rejected.

Following is the XML data format for authentication API:

```
<Auth uid="" rc="" tid="public|registered|mixed" ac="" sa="" ver="" txn="" lk="">
  <Uses pi="" pa="" pfa="" bio="" bt="" pin="" otp=""/>
  <Meta udc="" fdc="" idc="" cdc="" fpmi="" fpmc="" irmi="" irmc="" fdmi="" fdmc="" />
  <Skey ci="" ki="">encrypted and encoded session key</Skey>
  <Data type="X|P">encrypted PID block</Data>
  <Hmac>SHA-256 Hash of Pid block, encrypted and then encoded</Hmac>
  <Signature>Digital signature of AUA</Signature>
</Auth>
```

"Data" element contains "Pid" (Personal Identity Data) element which is a base-64 encoded encrypted block. Complete "Data" block should be encrypted at the time of capture on the client. But, encoding (base-64) of "Data" block and packaging it with enveloping XML under "Auth" element can either be done on the device or on the AUA server based on the AUA needs. Device capability, protocol between devices and AUA server, and data format used between devices and AUA server, etc. should be considered for making that choice.

When using PID block in XML format (which is the default), following is the format for "Pid" element:

```
<Pid ts="" ver="">
  <Demo lang="">
    <Pi ms="E|P" mv="" name="" lname="" lmv="" gender="M|F|T" dob="" dobt="V|D|A" age="" phone="" email=""/>
    <Pa ms="E" co="" house="" street="" lm="" loc="" 
        vtc="" subdist="" dist="" state="" country="" pc="" po=""/>
    <Pfa ms="E|P" mv="" av="" lav="" lmv=""/>
  </Demo>
  <Bios>
    <Bio type="FMR|FIR|IIR|FID" posh="" bs="">encoded biometric</Bio>
  </Bios>
  <Pv otp="" pin=""/>
</Pid>
```

Instead of XML format, this version also allows PID block to be in binary format based on Protocol Buffers standard ((http://code.google.com/p/protobuf/). Notice that "Auth" XML must be in XML format. Binary format is only supported for PID block to enable smaller packet sizes to be transmitted from devices. See Appendix for details.

3.3.1 Element Details

Element: **Auth** (mandatory)

- Root element of the input XML for authentication service.

Attributes:

- **uid** – (mandatory) Aadhaar Number of the resident
- **rc** – (mandatory) Resident consent to do the Aadhaar based authentication using OTP or Biometrics. Only allowed value is "Y". Without explicit informed consent of the Aadhaar holder AUA/Sub-AUA application should not call this API.
- **tid** – (mandatory) . For Public devices, value should be passed as "**public**". For Registered devices, value should be passed as "**registered**". In case of multi-factor biometric authentication if on factor is using registered and other factor is using public device value should be passed as "**mixed**". Additionally see Registered Devices section later in this document.
- **ac** – (mandatory) A unique code for the AUA which is assigned by UIDAI during AUA registration process. This is an alpha-numeric string having maximum length 10. (A Default value "public" is available which is ONLY for testing.)
- **sa** – (mandatory) A unique "Sub-AUA" code. AUAs are expected to manage these codes within their system and ensure uniqueness within their system.
    - This allows auditing and business intelligence to be provided at SA level. If AUA and SA are same agency, use value of "ac" for this attribute.
    - This is an alpha-numeric string having maximum length 10.
- **ver** – (mandatory) version of the API. Currently only valid value is "2.0".
- **txn** – (mandatory) AUA specific transaction identifier. AUA can choose to pass this as part of input. This is returned as part of response as is. This is very useful for linking transactions full round trip across systems.
    - This is an alpha-numeric string of maximum length 50. Only supported characters are A-Z, a-z, 0-9, period, comma, hyphen, backward & forward slash, left & right parenthesis, and colon. No other characters are supported.
    - It is highly recommended that AUAs use this attribute for correlating requests with responses for auditing and verification.
    - **In case of OTP Authentication using Request OTP API call this value of txn MUST be same as the txn value used for Request OTP API call**. This is to ensure OTP cannot be intercepted and used by other applications.
    - This **MUST NOT** start with **"U*:"** where "*" can be one or more alpha-numeric characters. All namespaces starting with "U" is reserved for various APIs offered by UIDAI.
- **lk** – (mandatory) A valid "License Key" assigned to the AUA. Administration portal of UIDAI will provide a mechanism for AUA administrator to generate license keys and use it within the authentication.
    - These license keys have expiry built into them and AUA administrator need to ensure that they generate new license keys before current ones expires through self-service portal.
    - This is an alpha-numeric string of length up to 64 characters.

Element: **Uses** (mandatory)

- This element specifies the authentication factors used by the request. When an authentication factor is specified in this element, that specific attribute must be present in the encrypted data block. This is particularly useful in situations where the AUA does not fully control the terminal device, but wishes to maintain a certain level of control on the authentication transaction.

Attributes:

- **pi** – (mandatory) Valid values are "y" or "n". If the value is "y" then at least one attribute of element "Pi" (part of "Demo" element) should be used in authentication. If value is "n", "Pi" element is not mandated.
- **pa** – (mandatory) Valid values are "y" or "n". If the value is "y" then at least one attribute of element "Pa" (part of "Demo" element) should be used in authentication. If value is "n", "Pa" element is not mandated.
- **pfa** – (mandatory) Valid values are "y" or "n". If the value is "y" then element "Pfa" (part of "Demo" element) should be used in authentication. If value is "n", "Pfa" element is not mandated.
- **bio** – (mandatory) Valid values are "y" or "n". If the value is "y" then at least one biometric element "Bio" (part of "Bios" element) should be used in authentication. If value is "n", "Bio" element is not mandated.
- **bt** – (mandatory only if "bio" attribute has value "y") provide a comma separated list of biometrics used. Valid values that can be used in this comma separated list are "FMR", "FIR", "IIR" and "FID". If "FMR" is part of the list, then at least one "Bio" element with type FMR should be used. Similarly, if "FIR" or "IIR" or "FID" are part of the list, then at least one "Bio" element with those types must be used.
- **pin** – (mandatory) Valid values are "y" or "n". If the value is "y" then PIN should be used in authentication. Otherwise, "pin" is not mandated.
- **otp** – (mandatory) Valid values are "y" or "n". If the value is "y" then OTP should be used in authentication. Otherwise, "otp" is not mandated.

Element: **Meta** (Mandatory)

This element specifies metadata related to the device and transaction. This is mandatory for better tracking, reporting, and trouble shooting. Additionally see Registered Devices section later in this document.

Attributes:

- **udc** – (mandatory) Unique Host/Terminal Device Code. This is a unique code for the host device assigned within the AUA domain. This is an alpha-numeric string of maximum length 20.
    - This allows better reporting and tracking of devices as well as help resolve issues at the device level.
    - It is highly recommended that AUAs define a unique codification scheme for all their devices.
    - Suggested format is *"[vendorcode][date of deployment][serial number]"*
- **fdc** – (mandatory) Fingerprint device code. This is an alpha-numeric string of maximum length 32. This is a unique code provided for the fingerprint sensor-

extractor combination. In the case of public devices, AUAs should obtain this code from sensor providers for certified sensors. In the case of registered devices, AUA application should call "getDeviceCode" function of the registered device and dynamically obtain the code.
    - While using fingerprint authentication, this code is mandatory and should be provided. If the code is unknown or device is not certified yet, use "NC".
    - For non-fingerprint authentication (when not using "bio" type "FMR" or "FIR"), use the value "NA".
- **idc** – (mandatory) Iris device code. This is an alpha-numeric string of maximum length 32. This is a unique code provided for the iris sensor-extractor combination. In the case of public devices, AUAs should obtain this code from sensor providers for certified sensors. In the case of registered devices, AUA application should call "getDeviceCode" function of the registered device and dynamically obtain the code.
    - While using iris authentication, this code is mandatory and should be provided. If the code is unknown or device is not certified yet, use "NC".
    - For non-iris authentication, use the value "NA".
- **cdc** – (mandatory) Camera device code. This is an alpha-numeric string of maximum length 32. This is a unique code provided for the face camera device. AUAs should obtain this code from the manufacturer. In the case of public devices, AUAs should obtain this code from sensor providers for certified sensors. In the case of registered devices, AUA application should call "getDeviceCode" function of the registered device and dynamically obtain the code.
    - While using face authentication, this code is mandatory and should be provided. If the code is unknown or device is not certified yet, use "NC".
    - For non-face authentication, use the value "NA".
- **fpmi** – (mandatory for registered device) Finger Print Manufacturer ID. If fingerprint device is a registered device then certified manufacturer should get an ID from UIDAI.
- **irmi** – (mandatory for registered device) Iris Manufacturer ID. If iris device is a registered device then certified manufacturer should get an ID from UIDAI.
- **fdmi** – (for registered device) Face device Manufacturer ID. If face camera device is a registered device then certified manufacturer should get an ID from UIDAI.
- **fpmc** – (mandatory for registered devices) For registered finger print device, this attribute holds signed public key certificate of the manufacturer. AUA application should call "getManufacturerCert" function of the registered device.
- **irmc** – (mandatory for registered device) For registered iris device, this attribute holds signed public key certificate of the manufacturer. AUA application should call "getManufacturerCert" function of the registered device.
- **fdmc** – (mandatory for registered device) For registered face camera device, this attribute holds signed public key certificate of the manufacturer. AUA application should call "getManufacturerCert" function of the registered device.

Element: **Skey** (mandatory)

- Value of this element is base-64 encoded value of encrypted 256-bit AES session key. **Session key must be dynamically generated for every transaction**

(session key must not be reused) and must not be stored anywhere except in memory. See next chapter for encryption details.

Attributes:

- **ci** – (mandatory) Public key certificate identifier using which "skey" was encrypted. UIDAI may have multiple public keys in field at the same time. Value of this attribute is the certificate expiration date in the format "YYYYMMDD". Expiry date of the certificate can be obtained from the certificate itself.
- **ki** – (optional) **This is for advanced use only**. Do not use this attribute unless you clearly understand what you are doing. See chapter on "API and Data Security" for details.

Element: **Data** (mandatory)

- Contains the encrypted "Pid" element in base-64 format. See "Pid" element definition later.

Attributes:

- **type** – (optional) Type of the PID block format. It can have two values – "X" for XML and "P" for Protobuf binary format. Default value is assumed to be "X".

Element: **Hmac** (mandatory)

- Devices which is constructing the "Pid" element must perform the following to provide the Hmac value:
  - If Pid type is "X" (XML), then:
    - After forming Pid XML, compute SHA-256 hash of Pid XML string
    - Then encrypt using session key (skey)
    - Then encode using base-64 encoding (as described earlier, encoding can be done on the AUA server when forming final Auth XML)
  - If Pid type is "P" (Protobuf), then:
    - After forming Protobuf byte array for Pid, compute SHA-256 hash of Pid protobuf bytes.
    - Then encrypt using session key (skey)
    - Then encode using base-64 encoding (as described earlier, encoding can be done on the AUA server when forming final Auth XML)

Authentication server performs the following processing on each authentication request:

1. Decode and Decrypt the Pid from Data element. Based on type attribute of the "Data" element, the value of Data is either interpreted as XML or Protobuf bytes.
2. Re-compute the SHA-256 Hash of Pid.
3. Decode and decrypt the value of Hmac element.
4. Compare the re-computed SHA-256 hash with Hmac value received in authentication request.
   a. If both values match, then, integrity of authentication request is preserved and server will proceed with further processing of the request.

b. If values do not match, reject the authentication request with error code representing "HMAC Validation failed".

Element: **Signature** (mandatory)

- The request XML should be digitally signed for message integrity and non-repudiation purposes.
- Digital signing should always be performed by the entity that creates the final request XML
  - AUA can digitally sign after forming the API input XML. This is almost always the case. In such cases, AUA ensures the message security and integrity between AUA servers and its client applications.
  - ASA can digitally sign the request XML if it is a domain-specific aggregator and forms the request XML on behalf of the AUA. In such cases, ASA and AUA ensure the message security and integrity between their servers.
- Procuring digital signature certificates:
  - It should be procured from a valid certification authority as per Indian IT Act (see http://cca.gov.in/rw/pages/faqs.en.do#thecaslicensedbythecca)
  - Digital certificates have two parts:
    - X.509 certificate representing public key.
    - Private Key which is used for digital signing. Private Key should be stored securely and is the responsibility of the owner of the certificate to ensure that it is not compromised.
  - It should be a class II or class III certificate.
  - X.509 certificate contains information about the owner of the certificate; in this case it will be details of the person and the organization to which he/she belongs. UIDAI server checks to ensure that certificate belongs to the ASA or AUA organization. Hence, it is mandatory that "O" attribute of "Subject" in the X.509 certificate matches the name of the organization.
- Digital signing of request XML
  - XML digital signature algorithm as recommended by W3C.
  - Signature should include key info element that contains X.509 certificate details. This is needed for UIDAI server to validate the signer.
- Verification of digital signature by UIDAI servers. UIDAI server validates the signature in the following sequence:
  - Checks if the signature element is present. If not, it throws an error.
  - If signature element is present, then it validates if the certificate is issued by one of the valid certification authority. If not valid, throws error.
  - If it is a valid certificate, then it validates whether the "O" attribute in the X.509 certificate's subject matches the AUA organization name. If yes, proceeds with API logic.
  - If it does not match AUA organization name, it checks configuration to see if ASA is allowed to sign on behalf of that AUA. If not, throws error.
  - If ASA is allowed to sign on behalf of that AUA, it checks whether the "O" element of the certificate matches with the organization name of the ASA. If not, throws error.
  - If it matches, it proceeds with API logic.
  - In future, UIDAI may choose to conduct additional validations against white listed certificates within UIDAI database.

Element: **Pid** (mandatory)

Attributes:

- **ts** – (mandatory) Timestamp at the time of capture of authentication input. This is in format "YYYY-MM-DDThh:mm:ss" (derived from ISO 8601). Time zone should not be specified and is automatically defaulted to IST (UTC +5.30). **Since timestamp plays a critical role, it is highly recommended that devices are time synchronized with a time server**.

AUAs can buffer authentication requests and send it to Aadhaar authentication server to support occasional lack of network connectivity on the field. Maximum time up to which requests can be queued (buffered) will be defined by UIDAI policy. Currently, this will be configured to 24 hours and may be changed as per policy. All requests with "ts" value older than this limit will be rejected.

When using SSK scheme or Registered Devices, this value is 4 hrs and all requests should be sent in same order as captured within 4 hours. Otherwise, requests will be rejected to ensure strong security.

- **ver** – (mandatory) version of the "Pid" element. Currently only valid value is "2.0" Notice that this is NOT same as Authentication API version. Pid version 1.0 is only for Authentication API versions 1.x.

Element: **Demo** (optional)

- Contains child elements "Pi", "Pa" and "Pfa", all of which are optional.
- All demographic data fields as per KYR specifications.

Attributes:

- **lang** – (optional) "Indian Language Code" in the case of using Indian language data for demographic match (see lname, lav attributes). This must be a valid language code from the following table

Language	Language code
Assamese	01
Bengali	02
Gujarati	05
Hindi	06
Kannada	07
Malayalam	11
Manipuri	12
Marathi	13
Oriya	15

Punjabi	16
Tamil	20
Telugu	21
Urdu	22

NOTE: Indian language matching of name and address allows data to be matched in any of the above languages using a fuzzy matching logic. In the case of address where multiple fields are provided as a single string (using "lav" attribute), it is recommended to separate each field (house, street, locality, vtc, district, etc) by comma.

Element: **Pi** (Optional)

- This element captures attributes related to "Personal Identity"

Attributes:

- **ms** – (optional) "Matching Strategy" for "name" attribute. Valid values are "E" (Exact match) and "P" (Partial match). This is used only for "name" attribute. Defaulted to "E".
- **mv** – (optional) "Match value" for "name" attribute. Valid values are the integers in the range 1 – 100 (inclusive). Default value is "100". "mv" attribute value MUST be specified when matching strategy ("ms" attribute) is "P".

  It represents the percentage of full words from the name stored in Aadhaar database that must be specified in the "name" attribute for the match to be considered successful. See examples below as part of "name" attribute description.

- **name** – (optional) Name of the resident in English. Maximum length is 60.

  NOTE: If "ms" and/or "mv" are provided, but, "name" attribute is not provided or empty value is provided, no name matching will be performed.

  When using matching strategy "Exact" (ms="E"), the name attribute is compared for exact match with the name stored in Aadhaar database. Though comparison is case insensitive, all the words of the name must be specified in the exact same order as provided by the resident during Aadhaar enrolment.

  When using matching strategy "Partial" (ms="P"), the name attribute is compared for partial match with the name stored in Aadhaar database based the following rules:

  1. Words from the name can appear in any order in the "name" attribute.
     For example: If resident's name is stored as "Anil Kumar Singh" in Aadhaar database, then, any of the inputs - "Kumar Anil Singh", "Anil Singh Kumar", "Singh Kumar Anil" or any other combinations – will result in successful match.

  2. Usage of specific titles is allowed in the "name" attribute. These are ignored for matching purposes. Supported titles are "Mr", "Mrs", "Dr", and "Ms". No other titles are currently supported.

For example: If resident's name is stored as "Anita Agarwal" in Aadhaar database, then, any of the inputs – "Dr. Anita Agarwal", "Ms. Anita Agarwal" or "Mrs Anita Agarwal" - will result in successful match,

3. Following special characters, if present in the "name" attribute, are ignored during matching:
    a. Period - (.)
    b. Comma (,)
    c. Hyphen (-)
    d. Asterisk (*)
    e. Opening and closing braces - '(' and ')'
    f. Opening and closing square brackets – '[' and ']'
    g. Apostrophes – `
    h. Single quotes – '
    i. Double quotes – "
    j. Forward slash - /
    k. Backward slash - \
    l. Hash - #
    m. Leading, trailing, and more than 1 contiguous spaces are removed before matching

    For example: If resident's name is stored as "Anita Agarwal" in Aadhaar database, then, "Agarwal, Anita" will result in successful match.

4. Input should not contain any additional words or initials that are not present in Aadhaar database. This will result in unsuccessful match and authentication failure.
    For example: If resident's name is stored as "Anita Agarwal" in Aadhaar database, then, "Anita Kumari Agarwal" or "Anita Kumari" or "Anita K Agarwal" will result in unsuccessful matches as the words "Kumari", "K" are not present in the Aadhaar database.

5. When used with "mv" value other than 100, then, inputs can have some words omitted or initials can be used in place a full word. The match is considered successful as long as input contains minimum number of matching full words as determined by the value of "mv".
    For example: Let us say that resident's name is stored as "Anil Kumar Singh" in Aadhaar database, and "mv" value is specified as 60 percent. It means at least 60% of total words must be matched. In the case of "Anil Kumar Singh", 60% of 3 (total words in name) is 1.8, rounded up to 2. Thus, any of the following inputs will result in successful match:
    a. "Anil Singh" – matches because of minimum 2 full words
    b. "Singh, Kumar Anil" – matches because of minimum 2 full words in any order and comma (,) is ignored.
    c. "Anil K Singh" – matches because of minimum 2 full words in any order and "K" is an initial of "Kumar".

    Following input will result in unsuccessful match:
    a. "Anil" – does not match because number of words is less than specified minimum.

b. "Anil K S" – does not match as initials are not counted as full words and hence, number of matching full words is less than specified minimum.
c. "Anil P Singh" – does not match as "P" is not an initial of any of the words stored in database.
d. "Anil S Singh" – does not match as after matching full words "Anil" and "Singh", "S" does not match as initial of "Kumar".

- **lname** – (optional) Resident's name in Indian language. This is a Unicode String in the language specified by the "lang" attribute of "Demo" element. Notice that this is a phonetic matching against the data stored in CIDR.

  NOTE: If this attribute is provided, "lang" attribute must be specified for "Demo" element.

- **lmv** – (optional) Local Language Match Value to adjust phonetic match threshold. This is a value between 1 and 100 (both inclusive).
- **gender** – (optional) Valid values are "M" for male, "F" for female, and "T" for transgender.
- **dob** – (optional) Date of Birth in "YYYY-MM-DD" format. If only year needs to be authenticated, then use format "YYYY".
- **dobt** – (optional) Date of Birth Type as indicated in Aadhaar system. This attribute can have only 3 values – "V" (for Verified), "D" (for Declared), and "A" (Approximate). When the resident is enrolled, DoB may be recorded along with any of these types.
- **age** – (optional) In certain use cases such as checking whether a resident can be considered a senior citizen or whether a resident is an adult (age above or equal to 18 years), it may be desired that only age of a resident can be verified using Aadhaar Authentication instead of verifying against complete data of birth. When "age" attribute is specified, authentication will pass if resident's age is "equal to or greater than" the input age. Else, it will fail with appropriate authentication error code.
- **phone** – (optional) Registered mobile phone number of the resident.
- **email** – (optional) Registered email address of the resident. This is case-insensitive match removing trailing and leading spaces.

Element: **Pa** (Optional)

- This element captures attributes related to "Personal Address". These are address fields as provided by the resident during enrolment or later updates. Only attributes that are sent as part of input will be compared.
- This element should not be used when using "Pfa" element as "Pa" and "Pfa" are mutually exclusive.

Attributes:

All attributes are compared case insensitive after leading and trailing spaces are trimmed and all the occurrences of consecutive spaces are replaced with single space.

- **ms** – (optional) "Matching Strategy" for address attributes. Only the value "E" (Exact match) is supported. This is used only when at least one address attribute is specified.
- **co** – (optional) "Care of" person's name.
- **house** – (optional) House identifier.
- **street** – (optional) Street name.
- **lm** – (optional) Landmark if any.
- **loc** – (optional) Locality where resident resides.
- **vtc** – (optional) Name of village or town or city.
- **subdist** – (optional) Sub-District name.
- **dist** – (optional) District name.
- **state** – (optional) State name.
- **country** – (optional) Country name.
- **pc** – (optional) Postal pin code.
- **po** – (optional) Post Office name.

Element: **Pfa** (Optional)

- This element captures attributes related to "Personal Full Address". It corresponds to the address of the resident as present in enrolment receipt or Aadhaar letter.
- This element should not be used when using "Pa" element as "Pa" and "Pfa" are mutually exclusive.

Attributes:

- **ms** – (optional) "Matching Strategy" for address attributes. Valid values are "E" (Exact match) and "P" (Partial match).
- **mv** – (optional) Valid values are integers in the range 1 -100 (inclusive). Default value is "100". It is used only when matching strategy (ms attribute) is "P" (Partial match).
  It represents the percentage of full words from the address stored in Aadhaar database that must be specified in the "av" attribute for the match to be considered successful,
- **av** – (optional) Resident's full address specified as a single string value.

  Normalization:
  "av" value and the resident's address stored in Aadhaar database, both are normalized using following rules before comparison.

  1. Following characters/phrases are ignored:
     a. Period - (.)
     b. Comma (,)
     c. Hyphen (-)
     d. Asterisk (*)
     e. Opening and closing braces - '(' and ')'
     f. Opening and closing square brackets – '[' and ']'
     g. Apostrophes – `

h. Single quotes – ‘
i. Double quotes – “
j. Forward slash - /
k. Backward slash - \
l. Hash - #
m. Care of labels – C/O, S/O, D/O, W/O, H/O
n. Other labels - “No.”

2. Leading and trailing spaces are trimmed and all the occurrences of multiple consecutive spaces are replaced with single space.

When using matching strategy “Exact” (ms=”E”), the normalized “av” attribute is compared for exact match with the normalized resident’s address stored in Aadhaar database.

When using matching strategy “Partial” (ms=”P”), the normalized “av” attribute is compared for partial match with the normalized resident’s address stored in Aadhaar database. Following are the rules of partial match:

1. Words can appear in any order.
2. Following additional normalizations are applied to both the “av” value and address stored in Aadhaar database:
   a. Commonly used words are replaced with their shortened version:
      I. “apartment” => “apt”
      II. “street” => “st”
      III. “road” => “rd”
      IV. “main” => “mn”
      V. “cross” => “crs”
      VI. “sector” => “sec”
      VII. “opposite” => “opp”
      VIII. “market” => “mkt”
   b. Suffixes typically used with numbers such as – st, nd, rd, th - are removed.
3. Example: 21st is converted to 21, 44th is converted to 44, etc. When used with “mv” value other than 100, some of the words can be omitted in the input. Match is considered successful if minimum number of full words that must match, as determined by the “mv” value, are present in the input.

Examples:
Scenario: Matching strategy “P”, mv=”60” (60%)

Given following value as resident’s address stored in database,

c/o A K Singh, Apartment #12, Lake view colony, Main street, Near Swimming pool, Rajajinagar, Bangalore, Karnataka, 560055

Following will be the normalized address.

a k singh apt 12 lake view colony main st near swimming pool rajajinagar bangalore karnataka 560055

Following are examples of matching and their result:

1. "*s/o A K singh, Lake view colony, apt #12, main st, Karnataka - 560055*" will be normalized to "*a k singh lake view colony apt 12 main st karnataka 560055*" – which results in successful match as 12 words are matched (more than 11 which is rounded 60% of total words 17).
2. "*s/o A K singh, Lake view colony Bangalore 560055" will be normalized to "a k singh lake view colony Bangalore 560055*" – which results in unsuccessful match since only 8 words are matched where as a minimum of 11 was requested (60% match value).

- **lav** – (optional) Resident's Address in Indian language. This is similar to "av" attribute described above except that this is represented in an Indian language. This will be matched against address data available in the CIDR database. If this attribute is provided, "lang" attribute must be specified for "Demo" element.
- **lmv** – (optional) Local Language Match Value to adjust phonetic match threshold. This is a value between 1 and 100 (both inclusive).

Element: **Bios** – (optional)
This element can have one or many "Bio" elements carrying biometric records to be matched.

Element: **Bio** (optional)
- If XML data format is used for PID block, this element contains single base 64 encoded biometric record. This is typically in plain ISO data format.
- In the case of registered devices, this contains encrypted FMR/FIR/IIR/FID record (see "Using Registered Devices" section later in the document).

Attributes:
- **type** – (mandatory) This attribute specifies type of the biometric. Valid values are "FMR" (Finger Minutiae), "FIR" (Finger Image), and "IIR" (Iris Image).
  - ***FMR*** - The biometric data is of type "Fingerprint Minutiae Record". This data is in ISO minutiae format with no proprietary extensions allowed.
  - ***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.
  - ***IIR*** - The biometric data is of type "Iris Image Record". The data is an iris image packaged in ISO 19794-6 format, which could contain a lossy compressed image having type Jpeg2000.
  - ***FID*** - The biometric data is of type "Face Image Data". The data is face image packaged in ISO 19794-5 format, which could contain a lossy compressed image having type Jpeg2000.
- **bs** – (mandatory for registered device) For registered device, Base-64 encoded signed biometric hash of the bio record. AUA application should call the registered device capture function to obtain the bio record as well as the signature string (bs).
- **posh** – (mandatory) In general, it is highly recommended that applications pass "UNKNOWN" unless it clearly knows which finger was used. Valid values are:

LEFT_IRIS
RIGHT_IRIS
LEFT_INDEX
LEFT_LITTLE
LEFT_MIDDLE
LEFT_RING
LEFT_THUMB
RIGHT_INDEX
RIGHT_LITTLE
RIGHT_MIDDLE
RIGHT_RING
RIGHT_THUMB
FACE
UNKNOWN

Element: **Pv** (optional)

- This element ("Pin Value") allows support for additional factors "pin" and "otp".

Attributes:

- **pin** – (optional) Actual value of PIN as set by resident. This attribute contains a 6 digit numeric value. **This option is NOT available for AUAs and is restricted to internal UIDAI usage only**.
- **otp** – (optional) This One Time Pin (OTP) value should be obtained from the Aadhaar holder.
    - To obtain OTP, following two ways can be used:
        - By the resident her/himself using resident portal, by sending an inbound SMS from registered phone, by calling IVR from registered phone, or by using UIDAI provided mobile app running on registered phone (TOTP).
        - By programmatically initiating the request from the AUA/sub-AUA application in which authentication is used. Whichever application needing to validate OTP can thus initiate OTP request on behalf of the resident via Request OTP API.

As per UIDAI security policy, if number of failed attempts crosses upper limit, Aadhaar record may be put on hold. The upper limit is dynamically computed based on various heuristics and is not a static number.

3.4 Authentication API: Response Data Format

Authentication API does not provide any identity data as part of the response. All it does is to match given input and respond with a "yes/no". Response XML is as follows:

```
<AuthRes ret="y|n" code="" txn="" err="" ts="" actn="" info="">
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha256" />
      <Reference URI="">
        <Transforms>
          <Transform
            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
        </Transforms>
        <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
        <DigestValue></DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue></SignatureValue>
  </Signature>
</AuthRes>
```

Agencies that use the authentication response need a mechanism to validate the authenticity of the authentication response for non-repudiation purposes. In order to enable verification and audit, authentication response will be digitally signed by UIDAI and the signature will be part of the response. AUAs are expected to preserve the entire response XML for non-repudiation purposes.

3.4.1 Element Details

Element: **AuthRes**

Attributes:

- **ret** – this is the main authentication response. It is either "y" or "n".
- **code** – unique alphanumeric "authentication response" code having maximum length 40. If the input is "not" processed due to errors such as decryption, wrong hmac value, etc., a value of "NA" will be returned. Once the integration is tested, this should not happen. But, due to some transmission errors or changes in deployments, if code is returned as "NA", AUAs may retry the transaction and if it continues to fail, may report to UIDAI technical support.
- **txn** – Authenticator specific transaction identifier. This is exactly the same value that is sent within the request.
- **ts** – Timestamp when the response is generated. This is of type XSD dateTime.
- **actn** – This attribute may or may not exist in response. This attribute, alpha-numeric of max length 5, provides specific action codes (published from time to time) **meant to be shown to resident/operator**. Refer to latest action codes at https://www.developer.uidai.gov.in/site/node/39
    - One possible use is to provide personalized resident feedback to improve authentication outcomes and required data update notifications.
    - **This attribute MUST be sent to front-end application by ASA/KSA and AUA/KUA to ensure action and corresponding message is displayed to resident/operator**.

- **info** – This attribute provides meta information on the details included in auth. This can be up to 128 characters and is composed of the following parts:

Version 3.0 structure of "info" (latest):

<Version>{SHA-256 of Aadhaar Number, SHA-256 of Demo element, Encoded Usage Data, pid_version, timestamp, fmrcount, fircount, iircount, fidcount, auth_api_ver, SHA-256 of ASA code, SHA-256 of AUA code, SHA-256 of SUB AUA code, lang, pi-ms, pi-mv, pi-lmv, pa-ms, pa-mv, pa-lmv, pfa-ms, pfa-mv, pfa-lmv, tid}

- "Version" – is the version of the info structure, "03"
- "SHA-256 of Aadhaar Number" – is the SHA-256 hash value of Aadhaar Number provided as part of input
- "SHA-256 of Demo Element" –
  - When Pid block is of type "X" (XML), then, it is the SHA-256 hash value of the substring representing Demo element in the Pid XML string.
  - When Pid block is of type "P" (Protobuf), then, it is the SHA-256 hash of the Protobuf value (byte array) of the Demo element.
- "Encoded Usage Data" - is 48 bit representation in HEX format of the various attribute usage of this authentication request.

  For version 3.0 of this block, Hexadecimal digits within the "Encoded Usage Data" should be interpreted based on below rules:

  1st hexadecimal digit:
  Bit 3-0: Version number of encoding. It will be hexadecimal "1" (binary: 0001) for encoding specified in this document.

  2nd hexadecimal digit:
  Bit 3: Was "`Pi->name`" attribute used?
  Bit 2: Was "`Pi->lname`" attribute used?
  Bit 1: Was "`Pi->gender`" attribute used?
  Bit 0: Was "`Pi->dob`" attribute used?

  3rd hexadecimal digit:
  Bit 3: Was "`Pi->phone`" attribute used?
  Bit 2: Was "`Pi->email`" attribute used?
  Bit 1: Was "`Pi->age`" attribute used?
  Bit 0: Was "`Pa->co`" attribute used?

  4th hexadecimal digit:
  Bit 3: Was "`Pa->house`" attribute used?
  Bit 2: Was "`Pa->street`" attribute used?
  Bit 1: Was "`Pa->lm`" attribute used?
  Bit 0: Was "`Pa->loc`" attribute used?

5th hexadecimal digit:
Bit 3: Was "`Pa->vtc`" attribute used?
Bit 2: Was "`Pa->dist`" attribute used?
Bit 1: Was "`Pa->state`" attribute used?
Bit 0: Was "`Pa->pc`" attribute used?

6th hexadecimal digit:
Bit 3: Was "`Pfa->av`" attribute used?
Bit 2: Was "`Pfa->lav`" attribute used?
Bit 1: Was "`FMR`" used for biometric auth?
Bit 0: Was "`FIR`" used for biometric auth?

7th hexadecimal digit:
Bit 3: Was "`IIR`" used for biometric auth?
Bit 2: Was "`FID`" used for biometric auth?
Bit 1: Was "`Pv->pin`" attribute used?
Bit 0: Was "`Pv->otp`" attribute used?

8th hexadecimal digit:
Bit 3: Was "`Pa->po`" attribute used?
Bit 2: Was "`Pa->subdist`" attribute used?
Bit 1: Was "`Pi->dobt`" attribute used?
Bit 0: Was "SSK" used?

9th hexadecimal digit::
Bit 3: Was "Pi->name" attribute matched?
Bit 2: Was "Pi->lname" attribute matched?
Bit 1: Was "Pi->gender" attribute matched?
Bit 0: Was "Pi->dob" attribute matched?

10th hexadecimal digit::
Bit 3: Was "Pi->phone" attribute matched?
Bit 2: Was "Pi->email" attribute matched?
Bit 1: Was "Pi->age" attribute matched?
Bit 0: Was "Pa->co" attribute matched?

11th hexadecimal digit::
Bit 3: Was "Pa->house" attribute matched?
Bit 2: Was "Pa->street" attribute matched?
Bit 1: Was "Pa->lm" attribute matched?
Bit 0: Was "Pa->loc" attribute matched?

12th hexadecimal digit::
Bit 3: Was "Pa->vtc" attribute matched?
Bit 2: Was "Pa->dist" attribute matched?
Bit 1: Was "Pa->state" attribute matched?
Bit 0: Was "Pa->pc" attribute matched?

13th hexadecimal digit::
Bit 3: Was "Pfa->av" attribute matched?
Bit 2: Was "Pfa->lav" attribute matched?
Bit 1: Was "FMR/FIR" matched for biometric auth?
Bit 0: Was "IIR" matched for biometric auth?

14th hexadecimal digit:
Bit 3: Was "Pa->po" matched for biometric auth?
Bit 2: Was "Pa->subdist" attribute matched?
Bit 1: Was "Pi->dobt" attribute matched?
Bit 0: Was "Registered" device used?

15th hexadecimal digit:
Bit 3: Currently unused. Will have value 0
Bit 2: Currently unused. Will have value 0
Bit 1: Currently unused. Will have value 0
Bit 0: Was "FID" matched for biometric auth?

- pid_version – Version string of the PID block which was part of input
- timestamp – PID "ts" string which was part of input
- fmrcount – Total number of FMR records which was part of input
- fircount – Total number of FIR records which was part of input
- iircount – Total number of IIR records which was part of input
- fidcount – Total number of FID records which was part of input
- auth_api_ver – Version string of auth XML which was part of input
- SHA-256 of ASA code – Hash value of the ASA code
- SHA-256 of AUA code – hash value of the AUA code
- SHA-256 of SUB-AUA code – Hash value of "sc" attribute of input
- lang – same as "lang" attribute of input. If input did not have it, this will contain value "NA".
- pi-ms – Match strategy used. Same as "ms" attribute of "Pi" element. If input did not have it, this will contain value "NA".
- pi-mv – Match value used. Same as "mv" attribute of "Pi" element. If input did not have it, this will contain value "NA".
- pi-lmv – Local language match value used. Same as "lmv" attribute of "Pi" element. If input did not have it, this will contain value "NA".
- pa-ms – Match strategy used. Same as "ms" attribute of "Pa" element. If input did not have it, this will contain value "NA".
- pa-lmv – Local language match value used. Same as "lmv" attribute of "Pa" element. If input did not have it, this will contain value "NA".
- pfa-ms – Match strategy used. Same as "ms" attribute of "Pfa" element. If input did not have it, this will contain value "NA".
- pfa-mv – Match value used. Same as "mv" attribute of "Pfa" element. If input did not have it, this will contain value "NA".
- pfa-lmv – Local language match value used. Same as "lmv" attribute of "Pfa" element. If input did not have it, this will contain value "NA".

- tid – P if public device, R if Registered device and M if Mixed device is used to capture biometrics.

  Example structure given below:

  ```
  03{f676e1becb2e308770ac5212acbbc7d93ba5693d828714a5136b
  6e1a9f438fc3,f25073ce9d46b0f720d00f32d8979c4efdab534686
  8ffac90f4412d02710f7ef,0100002020000000,2.0,20160603104
  809,1,0,0,0,2.0,1f5368b4cf6d7429033a47b8c7963329945c2bd
  f2690fa3685945b15d3cda2e0,96cae35ce8a9b0244178bf28e4966
  c2ce1b8385723a96a6b838858cdd6ca0a1e,,NA,P,50,NA,E,NA,NA
  ,NA,NA,NA,P}
  ```

- **err** – Failure error code. If authentication fails ("ret" attribute value is "n"), this attribute provides any of the following codes (for latest updates on error codes, see https://developer.uidai.gov.in/site/api_err):
  - **"100"** – "Pi" (basic) attributes of demographic data did not match.
  - **"200"** – "Pa" (address) attributes of demographic data did not match
  - **"300"** – Biometric data did not match
  - **"310"** – Duplicate fingers used
  - **"311"** – Duplicate Irises used.
  - **"312"** – FMR and FIR cannot be used in same transaction
  - **"313"** – Single FIR record contains more than one finger
  - "**314**" – Number of FMR/FIR should not exceed 10
  - "**315**" – Number of IIR should not exceed 2
  - "**316**" – Number of FID should not exceed 1
  - "**330**" – Biometrics locked by Aadhaar holder
  - "**400**" – Invalid OTP value
  - "**402**" – "txn" value did not match with "txn" value used in Request OTP API
  - **"500"** – Invalid encryption of Skey
  - **"501"** – Invalid certificate identifier in "ci" attribute of "Skey"
  - **"502"** – Invalid encryption of Pid
  - **"503"** – Invalid encryption of Hmac
  - **"504"** – Session key re-initiation required due to expiry or key out of sync
  - **"505"** – Synchronized Key usage not allowed for the AUA
  - **"510"** – Invalid Auth XML format
  - **"511"** – Invalid PID XML format
  - **"512"** – Invalid resident consent in "rc" attribute of "Auth"
  - **"520"** – Invalid device
  - **"521"** – Invalid FDC code under Meta tag
  - **"522"** – Invalid IDC code under Meta tag
  - **"523"** – Invalid CDC code under Meta tag
  - **"524**" – Invalid fpmi code under Meta tag
  - **"525"** – Invalid fpmc code under Meta tag
  - **"526"** – Invalid irmi code under Meta tag
  - **"527"** – Invalid irmc code under Meta tag
  - **"528"** – Invalid fdmi code under Meta tag
  - **"529"** – Invalid fdmc code under Meta tag

- **"530"** – Invalid authenticator code
- **"540"** – Invalid Auth XML version
- **"541"** – Invalid PID XML version
- **"542"** – AUA not authorized for ASA. This error will be returned if AUA and ASA do not have linking in the portal
- **"543"** – Sub-AUA not associated with "AUA". This error will be returned if Sub-AUA specified in "sa" attribute is not added as "Sub-AUA" in portal
- **"550"** – Invalid "Uses" element attributes
- **"551"** – Invalid "tid" value
- **"553"** – Registered devices currently not supported. This feature is being implemented in a phased manner.
- **"561"** – Request expired ("Pid->ts" value is older than *N* hours where *N* is a configured threshold in authentication server)
- **"562"** – Timestamp value is future time (value specified "Pid->ts" is ahead of authentication server time beyond acceptable threshold)
- **"563"** – Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA)
- **"564"** – HMAC Validation failed
- **"565"** – AUA license has expired
- **"566"** – Invalid non-decryptable license key
- **"567"** – Invalid input (this error occurs when some unsupported characters were found in Indian language values, "lname" or "lav")
- **"568"** – Unsupported Language
- **"569"** – Digital signature verification failed (means that authentication request XML was modified after it was signed)
- **"570"** – Invalid key info in digital signature (this means that certificate used for signing the authentication request is not valid – it is either expired, or does not belong to the AUA or is not created by a well-known Certification Authority)
- **"571"** – PIN Requires reset (this error will be returned if resident is using the default PIN which needs to be reset before usage)
- "**572**" – Invalid biometric position
- **"573"** – Pi usage not allowed as per license
- **"574"**– Pa usage not allowed as per license
- **"575"**– Pfa usage not allowed as per license
- **"576"** - FMR usage not allowed as per license
- **"577"** – FIR usage not allowed as per license
- **"578"** – IIR usage not allowed as per license
- **"579"** – OTP usage not allowed as per license
- **"580"** – PIN usage not allowed as per license
- **"581"** – Fuzzy matching usage not allowed as per license
- **"582"** – Local language usage not allowed as per license
- **"586"** – FID usage not allowed as per license. This feature is being implemented in a phased manner
- **"587"** – Name space not allowed
- **"588"** – Registered device not allowed as per license. This feature is being implemented in a phased manner
- **"590"** – Public device not allowed as per license
- **"710"** – Missing "Pi" data as specified in "Uses"

- **"720"** – Missing "Pa" data as specified in "Uses"
- **"721"** – Missing "Pfa" data as specified in "Uses"
- **"730"** – Missing PIN data as specified in "Uses"
- **"740"** – Missing OTP data as specified in "Uses"
- **"800**" – Invalid biometric data
- **"810"** – Missing biometric data as specified in "Uses"
- **"811"** – Missing biometric data in CIDR for the given Aadhaar number
- **"812"** – Resident has not done "Best Finger Detection". Application should initiate BFD application to help resident identify their best fingers. See Aadhaar Best Finger Detection API specification.
- **"820"** – Missing or empty value for "bt" attribute in "Uses" element
- **"821"** – Invalid value in the "bt" attribute of "Uses" element
- **"822"** – Invalid value in the "bs" attribute of "Bio" element within "Pid"
- **"901"** – No authentication data found in the request (this corresponds to a scenario wherein none of the auth data – Demo, Pv, or Bios – is present)
- **"902"** – Invalid "dob" value in the "Pi" element (this corresponds to a scenarios wherein "dob" attribute is not of the format "YYYY" or "YYYY-MM-DD", or the age of resident is not in valid range)
- **"910"** – Invalid "mv" value in the "Pi" element
- **"911"** – Invalid "mv" value in the "Pfa" element
- **"912"** – Invalid "ms" value
- **"913"** – Both "Pa" and "Pfa" are present in the authentication request (Pa and Pfa are mutually exclusive)
- **"930 to 939"** – Technical error that are internal to authentication server
- **"940"** – Unauthorized ASA channel
- **"941"** – Unspecified ASA channel
- **"950"** – OTP store related technical error
- **"951"** – Biometric lock related technical error
- **"980"** – Unsupported option
- **"995"** – Aadhaar suspended by competent authority
- **"996"** – Aadhaar cancelled (Aadhaar is no in authenticable status)
- **"997"** – Aadhaar suspended (Aadhaar is not in authenticatable status)
- **"998"** – Invalid Aadhaar Number
- **"999"** – Unknown error

4. API and Data Security

Broadly, Aadhaar authentication requests can be originated from either a "Registered" or a "Public" device. See registered Devices Specification for details of how they differ in working with biometric input.

4.1 Authentication Data Security

UIDAI provides a reference implementation of authentication client library for packaging and encrypting authentication data block in Java programming language. UIDAI may also provide other language implementations as necessary. Developers will be able to download these libraries along with UIDAI public key. Development community is encouraged to develop other programming language bindings and submit to UIDAI.

PID block data should be encrypted with a dynamic session key using **AES-256** symmetric algorithm (AES/ECB/PKCS7Padding). Session key, in turn, is encrypted with **2048-bit UIDAI public key** using asymmetric algorithm (RSA/ECB/PKCS1Padding). Reference implementation demonstrates this in detail. Session key must not be stored anywhere except in memory and should not be reused across transactions. Only re-use of session key that is allowed is its use as seed key when using synchronized session key scheme. To increase assurance multi-factor authentication using one-time pin (OTP) could also be used in conjunction with biometrics. See OTP API Specification for details on requesting OTP.

The encryption flow is as defined below:

1. Aadhaar Number, demographic, and biometric details as required by the application are entered into the device along with other factors such as OTP if it is used. If OTP is used, the request for OTP is sent to Aadhaar server along with Aadhaar Number (see "Aadhaar OTP Request API 1.6" specification). Aadhaar Authentication server sends the OTP back to the resident's registered mobile phone as an SMS and to the registered Email address.
2. AUA/Sub-AUA application generates a one-time session key.
3. The authentication "Data" XML block is encrypted using the one-time session key and then encoded (base 64).
4. The session key is then encrypted with the UIDAI public key.
5. AUA application on the device sends the encrypted block along with HMAC data to AUA server.
6. AUA server forms the final authentication XML input for API including license key, transaction reference ("txn" attribute), and sends the data to Aadhaar authentication server through an ASA network.
7. Aadhaar authentication server decrypts session key with the UIDAI private key. The data block is then decrypted using the session key.
8. The resident's decrypted biometric, demographic information, and optional OTP is taken into account during match based on the input.

9. Aadhaar authentication server responds with a "yes/no" as part of the digitally signed response XML.

4.2 Using Registered Devices

This authentication 2.0 API supports Registered Devices in addition to Public devices. Registered devices enhances biometric capture security by ensuring capture is necessarily done within a certified device. For more information on registered devices for manufacturers, refer to the specification document available at http://uidai.gov.in/images/aadhaar_registered_devices_2_0.pdf

4.3 Using Synchronized Session Key

As an advanced feature, this revision of the API version also supports a scheme called Synchronized Session Key. This allows session key to be sent in the beginning of the session and subsequent keys not to be sent for up to expiry of the session. At a high level, logic is as follows:

1. Authentication client generates an AES session key, generates a unique session identifier (key identifier) and sends the authentication request along with session key encrypted with PKI. Let's call it "seed" key.
2. For subsequent transactions within the maximum session expiry time (4 hours), authentication client does the following:
    a. Generate a new random number (CSPRNG) and generate a new AES key using the seed session key and this random number
    b. Send the authentication request along with the random number and key identifier without actually sending new session key
3. When seed session key expires (either 4 hours have passed since original session key was sent or server sends a 504 error), start with step 1.

4.4 Using Binary format for PID block

Protocol Buffers are a way of encoding structured data in an efficient yet extensible format. Google uses Protocol Buffers for almost all of its internal RPC protocols and file formats. It provides a flexible, efficient, automated mechanism for serializing structured data. See https://developers.google.com/protocol-buffers/docs/overview for details.

This version of the API supports PID block to be sent to AUA server in protobuf format as an alternate to default XML format. This allows compact binary representation of the device data and avoids extra encoding required for XML format. If this scheme is used, device applications are expected to form the PID block in protobuf format using the ".proto" file for PID block. Final ".proto" files for this version are available at https://developer.uidai.gov.in/site/downloads

4.5 Authentication Audits

Aadhaar authentication will record all the authentication requests and their responses for audit purposes. By providing the Aadhaar number and authentication response code ("code" attribute in "AuthRes"), AUAs can request UIDAI to confirm the result of an authentication and authentication factors that were presented in that authentication request. UIDAI policy will determine how long these audits are maintained within CIDR.

All authentication responses are digitally signed by UIDAI and AUA's are recommended to validate the response integrity the keep track of these for audit purposes. In addition, attributes "ts", "info" within the API response can be used to verify if it the request was indeed for a particular Aadhaar number, if the request indeed had a biometric factor, when was the authentication done, etc. Such self-verifiability of the authentication response allows 3rd party applications to trust and electronically verify the digitally signed response quite similar to that of an offline trust establishment against a gazetted officer signed paper.

5. Appendix

5.1 Related Publications

Demographic Data Standards	http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
Biometric Standards	http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf
Aadhaar biometric APIs	http://uidai.gov.in/UID_PDF/Working_Papers/Aadhaar_ABIS_API.pdf
Data Encryption Algorithm	ANXI X3.92
Banking—Retail Financial Services Symmetric Key Management	ANSI X9.24
Public Key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Cryptography	ANSI X9.42
Triple Data Encryption Algorithm: Modes of Operation	ANSI X9.52
Security Requirements for Cryptographic Modules	FIPS PUB 140-2
Personal Identification Number (PIN) Management and Security	ISO 9564
Information Technology – Security Techniques – Hash Functions	ISO 10118
Information Technology – Security Techniques – Key Management	ISO 11770
Information Technology – Security Techniques – Encryption Algorithms	ISO 18033
Biometric standards	ISO 19794-4, ISO 19794-6
Date and Time format standard	ISO_8601
XML Signature	http://www.w3.org/TR/xmldsig-core/
Indian e-governance standard for Metadata and Data standards for Person and Land Region codification	http://egovstandards.gov.in/standardsandFramework/metadata-and-data-standards/MDDS_Standard_release_version_1.0__Dec_24_2k9.pdf
Protocol Buffers	http://code.google.com/p/protobuf/
Geo Location Standard	ISO 6709

5.2 Changes in Version 2.0 from Version 1.6

New (2.0)
Resident consent for authentication
Txn attribute naming convention clarified further
Additional support of signed biometrics as part registered devices support within PID block
Meta element has additional attributes to support registered devices
Geo location, public IP details removed Meta element
Country added in “pa” element within PID block
Info attribute of the response enhanced for version 2.0 to 3.0
“actn” attributed added in the response
Additional error codes added

AUA Audit Compliance Checklist

Unique Identification Authority of India

SNo	Compliance	Yes	No
A1	**Security Framework Policies for AUA- Mandatory**		
1	For better decoupling and independent evolution of various systems, it is necessary that Aadhaar number be never used as a domain specific identifier. In addition, domain specific identifiers need to be revoked and/or re-issued and hence usage of Aadhaar number as the identifier does not work since Aadhaar number is permanent lifetime number. **Example:** Instead of using Aadhaar number as bank customer id or license number or student id, etc., always have a local, domain specific identifier and have the mapping in the backend database		
2	In the case of assisted devices and applications where operators need to mandatorily perform application functions (not a self-service application), operators should be authenticated using some authentication scheme such as password, Aadhaar authentication, smart card based authentication, etc.		
3	PID block captured for Aadhaar authentication must be encrypted during capture and should never be sent in the clear over a network.		
4	The encrypted PID block should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted		
5	Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database		
6	The meta data and the responses shall be stored for audit purposes for over a period of time (minimum 6 months)		
7	It is mandatory that network between AUA and ASA be secure. It is strongly recommended to have leased lines or similar secure private lines between ASA and AUA. If a public network is used, a secure channel such as SSL should be used.		
A 2	**Security Framework Policies for Authentication Devices- Mandatory**		
8	PID block captured for Aadhaar authentication must be encrypted during capture and should never be sent in the clear over a network		
9	The encrypted PID block should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted. Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database		
10	In the case of assisted devices and applications where operators need to mandatorily perform application functions (not a self-service application), operators should be authenticated using some authentication scheme such as password, Aadhaar authentication, smart card based authentication, etc		
11	In terms of data storage, authentication devices must comply with all applicable laws and regulations of the country like IT Act		
B1	**Security Framework Policies for AUA- Recommended**		
12	It is recommended to deploy digitally signed applications on the devices with some AUA specific mechanism to identify trusted devices and applications. For device authentication, digital certificate or other mechanisms may be used.		
13	It is recommended that all AUAs follow standards such as ISO 27000 to maintain Information security. AUAs and their partners who participate in conducting Aadhaar authentication should ensure compliance to prevailing		

SNo	Compliance	Yes	No
	laws such as IT Act		
14	Software to prevent malware/virus attacks may be put in place and anti-virus software installed to protect against viruses. Additional networks security controls and end point authentication schemes may be put in place.		
15	It is recommended that some periodic standard certification and audit process be established for applications, devices, and overall networks across the ecosystem and also to ensure the compliance to standard security policy and procedure.		
16	It is highly recommended that the AUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analysing authentication related transactions to identify fraud cases and patterns		
B2	**Security Framework Policies for Authentication Devices- Recommended**		
17	Wherever possible, only the domain specific identifier should be captured at the device end and not the Aadhaar number. For e.g. — Wherever possible, AUAs should only capture their domain specific identifier (bank a/c no, ration card no along with family member id, LPG customer account no, etc.) — On the AUA server, when forming the authentication input XML, retrieve the Aadhaar number from AUA database using domain specific identifier		
	A trusted environment must be created at the device side		
18	It is recommended that some periodic standard certification and audit process be established for applications, devices, and overall networks across the ecosystem and also to ensure the compliance to standard security policy and procedure		
19	Additional factors may be used to strengthen authentication of operators, devices, and residents wherever needed		
C	**XML Signature Syntax & processing – Recommendations by W3C**		
20	http://www.w3.org/TR/xmldsig-core/		
D	**Audit logging requirements**		
21	Authentication audit trail should be for a minimum of 6 months Auditable fields - API Name, AUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-PII data.		
E	**Aadhaar Authentication API Specification 1.6**		
22	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf		
F	**Best Finger Detection API Specification 1.6**		
23	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf		
G	**OTP Request API Specification 1.5**		
24	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf		
H	**Biometric Devices Specifications for Aadhaar Authentication**		
25	http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf		
I	**Demographic Data Standards**		
26	http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf		
J	**Biometric Data Interchange Standards**		
27	ISO/IEC 19794-2:2005, ISO/IEC 19794-4:2005		

SNo	Compliance	Yes	No
K	**Date & Time Format Standards**		
28	ISO_8601		

☐ **I hereby declare that the above requirements have been audited and meet the UIDAI standards & specifications**

Auditor Name: _____

Auditor Signature: _____

Date: _____

Seal: _____

Unique Identification Authority of India

AUA Go Live Checklist

Sr No	Activities	AUA
1	AUA has arranged for infrastructure for digital signature and tested in Pre-production environment	☐
2	The Public key corresponding to Digital signature infrastructure submitted to UIDAI	☐
3	The format of public key is X.509	☐
4	AUA has conducted end-to-end testing for 100 no of successful transactions in Pre-production environment	☐
5	AUA data logging for Authentication Audit trail being provisioned	☐
6	AUA is ready to deploy devices with STQC certified sensor-extractor, if using biometric authentication and FDC code(s) have been arranged (Refer Aadhaar Authentication API Document, pg 14 & 15)	☐
7	UDC Nomenclature Defined	☐
8	Domain Application is ready for deployment	☐
9	Client Application has provisioned for BFD, two Finger Authentication, UDC, Location configuration and Operator login in case of operator assisted devices. (Refer Aadhaar Authentication & BFD API)	☐
10	Obtained certificate from an information systems auditor certified by a recognized body for compliance to UIDAIs standards and specifications	☐
11	Resident consent process to obtain consent is ready to be deployed	☐

*All the above items are mandatory and need to be completed before submitting for go live approval to UIDAI

AUA hereby confirms compliance to the current standards and specifications as published by UIDAI.

Submitted By *(from AUA Organization)*
Signature: _____
Name: _____
Designation: _____
Organization: _____
Date: _____

Approved By *(from UIDAI)*
Signature: _____
Name: _____
Designation: _____
Organization: _____
Date: _____

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India,
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

AADHAAR E-KYC SERVICE

NOVEMBER 2012

Table of Contents

ABBREVIATIONS **3**

1. INTRODUCTION **4**

1.1 AADHAAR ENROLMENT ECOSYSTEM 5
1.2 AADHAAR UPDATION ECOSYSTEM 5
1.3 AADHAAR AUTHENTICATION ECOSYSTEM 6
1.4 AADHAAR E-KYC ECOSYSTEM 6

2. FEATURES OF THE AADHAAR E-KYC SERVICE **7**

2.1 SALIENT FEATURES OF THE E-KYC SERVICE 7
2.2 COMPLIANCE WITH THE INFORMATION TECHNOLOGY ACT, 2000 8
2.3 DEPLOYMENT OF THE AADHAAR E-KYC SERVICE 8

3. AADHAAR E-KYC OPERATING MODEL **10**

3.1 AADHAAR AUTHENTICATION 10
3.2 STAKEHOLDERS 10
3.3 E-KYC DATA FLOW 11
3.4 PRICING OF E-KYC TRANSACTIONS 12

4. INSTANT SERVICE DELIVERY WITH E-KYC **13**

4.1 INSTANT SERVICE PROVISIONING 13
4.1.1 Government applications 13
4.1.2 Other applications 14
4.2 AADHAAR AS A PAYMENT ADDRESS 15

5. CONCLUSION **17**

Abbreviations

API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
CIDR	Central ID Data Repository
e-KYC	Electronic Know Your Customer
FI	Financial Inclusion
IT	Information Technology
KSA	KYC Service Agency
KUA	KYC User Agency
OTP	One Time PIN
RBI	Reserve Bank of India
STQC	Standardisation Testing and Quality Certification Directorate
UIDAI	Unique Identification Authority of India

1. Introduction

The Unique Identification Authority of India (UIDAI) has been established with the mandate of providing a Unique Identification Number (Aadhaar) to all residents of India[1]. The UIDAI has now issued Aadhaar to over 20 crore residents of India. During enrollment, the following data is collected:

1. Demographic details[2] such as the name of the resident, address, date of birth, and gender;
2. Biometric details[3] such as the fingerprints, iris scans[4], and photograph; and
3. Optional fields for communication of such as the mobile number and email address.

The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity biometrically[5] through presentation of their fingerprints or non-biometrically using a One Time Password (OTP) sent to the registered mobile phone or e-mail address. Iris authentication[6] will soon be launched by the UIDAI.

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a key requirement for access to financial products (payment products, bank accounts, insurance products, market products, etc.), purchasing SIM cards for mobile telephony, buying LPG, and access to various Central, State, and Local Government services. Today, customers provide physical PoI and PoA documents. Aadhaar is already valid KYC for banking[7], insurance[8], capital markets[9], telecom[10], LPG[11], Railways[12], and various Government services. In addition, the UIDAI now also proposes to provide an e-KYC service, through which the KYC process can be performed electronically with explicit authorization by resident. **As part of the e-KYC process, the resident authorizes UIDAI (through Aadhaar authentication using either biometric/OTP) to provide their demographic data along with their photograph (digitally signed and encrypted) to service providers**. The e-KYC service has the potential to revolutionize service delivery in the public and private sector, and drive innovation in the market.

[1] http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf
[2] http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
[3] http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf
[4] http://uidai.gov.in/UID_PDF/Working_Papers/UID_and_iris_paper_final.pdf
[5] http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf
[6] http://uidai.gov.in/images/iris_poc_report_14092012.pdf
[7] http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7367
[8] http://www.irda.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo1322&flag=1
[9] http://www.sebi.gov.in/cms/sebi_data/attachdocs/1344851126270.pdf
[10] http://www.dot.gov.in/as/2011/as_14.01.2011.pdf
[11] http://uidai.gov.in/images/FrontPageUpdates/aadhaar_news_release_28_june.pdf
[12] http://www.indianrail.gov.in/id_proof.doc

Service providers can provide a paperless KYC experience by using e-KYC and avoid the cost of repeated KYC, the cost of paper handling and storage, and the risk of forged documents. The real-time e-KYC service makes it possible for service providers to provide instant service delivery to residents, which otherwise would have taken a few days for activation based on the verification of KYC documents, digitization, etc.

1.1 Aadhaar enrolment ecosystem

The Aadhaar enrolment ecosystem[13] consists of Registrars appointed by UIDAI, who in turn appoint Enrolment Agencies, who in turn appoint certified operators. In co-ordination with the Registrars, the Enrolment Agencies set up enrolment centres, where residents can enrol for Aadhaar. Multiple fingerprint scanners, iris scanners, and cameras used for enrolment are certified[14] by STQC and UIDAI, and all connect to the UIDAI designed enrolment client through a standard Application Programming Interface (API)[15]. This makes it possible for Enrolment Agencies to use any certified equipment.

Appointment of multiple registrars, multiple enrolment agencies, and multiple technology providers has created an environment of healthy competition, which has brought about speed and kept costs under control in addition to providing choice. This ecosystem has enrolled over 20 crore residents for Aadhaar in a period of two years.

1.2 Aadhaar updation ecosystem

The UIDAI has published an updation policy[16], which lays the foundation for residents to update their data in the UIDAI database. Residents can update their data (such as residential address, mobile number, email for example) at a permanent updation centre, or through the website.

Given that the Aadhaar will become the foundation for service delivery in the public and private sector, residents will have the incentive to keep their data updated with the UIDAI at all times. Alignment of this incentive for efficient service delivery demanded by residents, with the need for accurate data by Government will ensure that the Aadhaar database becomes the authoritative database for service delivery.

[13] http://uidai.gov.in/registrar-link-2.html
[14] http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification
[15] http://uidai.gov.in/UID_PDF/Working_Papers/UID_Biometrics_Capture_API_draft.pdf
[16] http://uidai.gov.in/images/update_policy_version_2_1.zip

1.3 Aadhaar authentication ecosystem

The UIDAI has set up a scalable ecosystem for the purpose of instant authentication[17] of residents. The UIDAI has appointed a number of Authentication Service Agencies (ASAs), who in turn are appointing various Government and non-Government organizations as Authentication User Agencies (AUAs). The UIDAI, in partnership with STQC, has also laid down the technical standards for biometric devices, and certified[18] a number of them. Since the authentication service is provided online and in real-time, the UIDAI has also established two data centres where authentication and other online services such as e-KYC are deployed in active-active mode to ensure high availability.

The Aadhaar authentication ecosystem is capable of handling tens of millions of authentications on a daily basis, and can be scaled up further as demand increases. Banks and payment network operators have embedded Aadhaar authentication into microATMs[19] in order to provide branch-less banking anywhere in the country in a real-time, scalable, interoperable manner.

1.4 Aadhaar e-KYC ecosystem

A fundamental building block for service delivery is the KYC (Know Your Customer) process, which establishes the identity of the resident, their address, and other basic information such as their date of birth and gender. Typically, this KYC information is combined with other information at the point of service delivery to determine eligibility – either for an LPG connection, a scholarship, a loan, a social security pension, a mobile connection, etc.

The Aadhaar e-KYC service provides an instant, electronic, non-repudiable proof of identity and proof of address along with date of birth and gender. In addition, it also provides the resident's mobile number and email address to the service provider, which helps further streamline the process of service delivery. E-KYC may be performed at an agent location using biometric authentication, as well as remotely using an OTP on a website or mobile connection.

The Aadhaar e-KYC ecosystem has been designed to be scalable, just like the enrolment, updation, and the authentication ecosystems. It follows the same operating model as that of the Aadhaar authentication ecosystem.

The rest of this document describes the e-KYC service and ecosystem in detail.

[17] http://uidai.gov.in/auth.html
[18] http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification
[19] http://www.iba.org.in/Documents/MicroATM_Standards_v1.5_FINAL_Aug11_2012[1].pdf

2. Features of the Aadhaar e-KYC service

2.1 Salient Features of the e-KYC service

1. **Paperless**: The service is fully electronic, and document management can be eliminated.

2. **Consent based**: The KYC data can only be provided upon authorization by the resident through Aadhaar authentication, thus protecting resident privacy.

3. **Eliminates Document Forgery**: Elimination of photocopies of various documents that are currently stored in premises of various stakeholders reduces the risk of identity fraud and protects resident identity. In addition, since the e-KYC data is provided directly by UIDAI, there is no risk of forged documents.

4. **Inclusive**: The fully paperless, electronic, low-cost aspects of e-KYC make it more inclusive, enabling financial inclusion.

5. **Secure and compliant with the IT Act**: Both end-points of the data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper documents. In addition, the use of encryption and digital signature ensures that no unauthorized parties in the middle can tamper or steal the data.

6. **Non-repudiable**: The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital signature by UIDAI when providing the e-KYC data makes the entire transaction non-repudiable by all parties involved.

7. **Low cost**: Elimination of paper verification, movement, and storage reduces the cost of KYC to a fraction of what it is today.

8. **Instantaneous**: The service is fully automated, and KYC data is furnished in real-time, without any manual intervention.

9. **Machine Readable**: Digitally signed electronic KYC data provided by UIDAI is machine readable, making it possible for the service provider to directly store it as the customer record in their database for purposes of service, audit, etc. without human intervention making the process low cost and error free.

10. **Regulation friendly**: The service providers can provide a portal to the Ministry/Regulator for auditing all e-KYC requests. The Ministry/Regulator can establish rules for secure retention of e-KYC data (eg. storage method, period of storage, and retrieval among other things).

2.2 Compliance with the Information Technology Act, 2000

The data provided to the service provider is fully in compliance with the Information Technology Act (IT Act), 2000[20] as follows:

1. The e-KYC electronic record provided by UIDAI is equivalent to the Aadhaar letter (Section 4 of the IT Act, 2000);

2. A cryptographic hash of the KYC data is computed and attached with. The SHA-2 digital hash function algorithm is used. Hashing ensures that any tampering of the data in transit is detected (Section 3 of the IT Act, 2000);

3. The KYC data along with the computed hash are encrypted using a combination of AES-256 symmetric key and RSA-2048 PKI encryption form a secure electronic record. The encryption ensures that only the intended service provider can view the data provided by UIDAI (Section 14 of the IT Act, 2000); and

4. The encrypted data and hash are digitally signed by UIDAI using RSA-2048 PKI. The secure digital signature of UIDAI can be verified by the service provider to ensure the authenticity of the source (Section 15 of the IT Act, 2000).

The e-KYC service is compliant with the latest standards notified in the *Information Technology (Certifying Authorities), Amendment Rules 2011 – 25th October 2011(GSR 782(E) & GSR 783(E)-Standards (Hash & key Size), usage period of private keys, verification of Digital Signature Certificate*[21].

2.3 Deployment of the Aadhaar e-KYC service

The Aadhaar e-KYC API[22] 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).

[20] http://deity.gov.in/content/information-technology-act
[21] http://deity.gov.in/sites/upload_files/dit/files/GSR782_GSR783_08112011(1).pdf
[22] http://uidai.gov.in/images/aadhaar_kyc_api_1_0_170912.pdf

Broadly speaking, two scenarios under which the e-KYC service can be used:

1. **New customer/beneficiary**:
    a. The KUA captures resident authentication data and invokes the Aadhaar e-KYC API through a KSA network;
    b. The KYC data returned within the response of the e-KYC API is digitally signed and encrypted by UIDAI; and
    c. Using the resident data obtained through this KYC API, the agency can provision the service instantaneously.

2. **Existing customer/beneficiary**
    a. The KUA captures resident authentication data and invokes the Aadhaar e-KYC API through a KSA network;
    b. The KYC data returned within the response of the e-KYC API is digitally signed and encrypted by UIDAI;
    c. Since the resident is already a customer/beneficiary, the KUA can use a simple workflow to approve the Aadhaar linkage by comparing data retrieved through the e-KYC API against what is on record (in paper or electronic form); and
    d. Once verified, the existing customer/beneficiary record can be linked to the Aadhaar number.

The Aadhaar e-KYC API returns data along with a unique transaction code. The fact that the data is digitally signed by UIDAI and that every transaction has a unique code makes it possible to perform an electronic audit at a later point in time for any particular transaction.

The Aadhaar e-KYC service does not compromise security for inclusion, and instead offers a solution that is secure as well as inclusive and protects data privacy by eliminating paper trail on the field.

3. Aadhaar e-KYC operating model

The Aadhaar e-KYC service has been designed as a layer on top of the Aadhaar authentication service. Thus, it uses an operating model that is very similar to that of Aadhaar authentication[23].

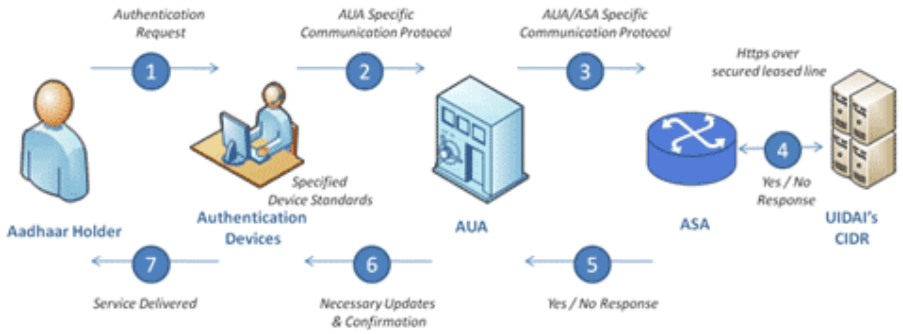
3.1 Aadhaar authentication

Aadhaar authentication is a process where the Aadhaar number, along with other attributes (demographic/biometrics/OTP) are submitted to UIDAI's Central Identities Data Repository (CIDR) for verification. The CIDR verifies whether the data submitted matches the data available in CIDR and responds with either a yes or a no.

3.2 Stakeholders

The UIDAI authentication ecosystem consists of a number of stakeholders, which also holds true for the e-KYC ecosystem:

Figure 1: The Aadhaar authentication ecosystem



1. **Unique Identification Authority of India (UIDAI):** UIDAI is the overall regulator and overseer of the Aadhaar authentication system. It owns and manages the Central Identities Data Repository (CIDR) that contains the personal identity data (PID) of all Aadhaar-holders.
2. **Authentication Service Agency (ASA):** ASAs are entities that have secure leased line connectivity with the CIDR. ASAs transmit authentication requests to CIDR on behalf of one or more AUAs. An ASA enters into a formal contract with UIDAI.

[23] http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

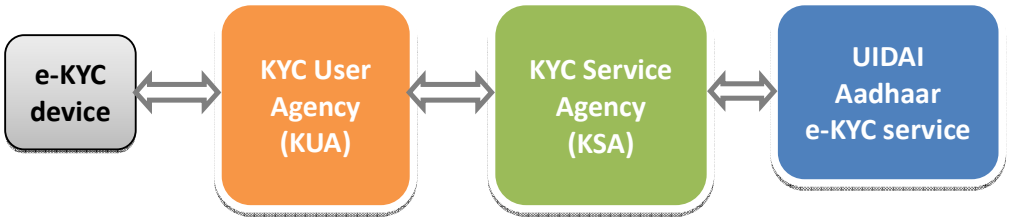
3. **Authentication User Agency (AUA):** An AUA is any entity that uses Aadhaar authentication to enable its services and connects to the CIDR through an ASA. An AUA enters into a formal contract with UIDAI.
4. **Sub AUA:** An entity desiring to use Aadhaar authentication to enable its services through an existing AUA. Examples: (i) The IT Department of a State/UT could become an AUA and other departments could become its Sub AUAs to access Aadhaar authentication services. (ii) A Hoteliers Association becomes an AUA and several hotels could access Aadhaar authentication as its Sub AUAs. UIDAI has no direct contractual relationship with Sub AUAs.
5. **Authentication Device Technology Service Provider:** These are the devices that collect PID (Personal Identity Data) from Aadhaar holders, transmit the authentication packets and receive the authentication results. Examples include PCs, kiosks, handheld devices etc. They are deployed, operated and managed directly by the AUA/Sub AUA, or through a Technology Service Provider.
6. **Aadhaar holders:** These are holders of valid Aadhaar numbers who seek to authenticate their identity towards gaining access to the services offered by the AUA.

The key stakeholders could engage with each other in multiple ways. For example, an AUA could choose to become its own ASA, an AUA could access Aadhaar authentication services through multiple ASAs for reasons such as business continuity planning, an AUA transmits authentication requests for its own service delivery needs as well as on behalf of multiple Sub AUAs, .

Similarly, it may also be possible to use a single authentication device for servicing multiple AUAs. For example, the authentication device at a fair price shop may also be used for carrying out financial transactions for banks.

3.3 e-KYC data flow

Currently, all ASAs and AUAs are approved by the UIDAI to access the e-KYC service. Hence, every ASA is also a KYC Service Agency (KSA), and every AUA is also a KYC User Agency (KUA). The following diagram depicts the relationship between various entities in the e-KYC transaction. The operating model for e-KYC is the same as that for authentication.



The data flow for an e-KYC is as follows:

1. The e-KYC front-end application captures Aadhaar number along with the biometric/OTP of resident and forms the encrypted PID block;
2. The KUA forms the e-KYC XML by encapsulating the PID block, affixes the digital signature and sends it to the KSA (the digital signature step can be delegated by the KUA to the KSA);
3. The KSA forwards the e-KYC XML (affixing the digital signature if delegated by the KUA to the KSA) to UIDAI's Aadhaar KYC service;
4. The Aadhaar KYC service authenticates the resident. If the authentication is successful, it responds back with a digitally signed and encrypted demographic and photograph in XML format;
5. The demographic data and photograph in response is encrypted by default with the KUA's encryption key. Upon the KUA's request, this may be instead encrypted with the key of the KSA; and
6. The KSA sends the response back to KUA, which interprets the result for service delivery.

3.4 Pricing of e-KYC transactions

E-KYC Services are offered free of cost as of now, till a pricing policy decision is announced.

4. Instant service delivery with e-KYC

The Aadhaar e-KYC service can help drive instant service delivery in the following ways:

1. Instant service provisioning on the basis of e-KYC in the public and private sector;
2. Enable the use of Aadhaar as a payment address; and
3. Enable combination product offerings at one location, which would have otherwise required the resident to make multiple trips to multiple locations.

4.1 Instant service provisioning

The Aadhaar e-KYC service can be used for instant service provisioning wherever KYC details are required. In some cases, the KYC requirements are regulatory, whereas in other cases, the KYC requirements are for the purpose of getting basic customer data for service provisioning.

4.1.1 Government applications

The Aadhaar e-KYC service can help speed up the realization of the goals of the Electronic Service Delivery Bill[24]. A key application of e-KYC in Government applications is the seeding of Aadhaar in the various Government Schemes for service delivery.

The Budget Speech 2012-13 (Paragraph 124)[25] identified the need for Aadhaar-based payments for MGNRES wages, old age, widow, and disability pensions, and various education scholarships. The Prime Minister has recently constituted a National Committee on Direct Cash Transfers[26] under his chairmanship and an Executive Committee on Direct Cash Transfers to give a thrust to roll out a cash transfer programme across the country, leveraging the Aadhaar platform. The Task Force on Direct Transfer of Subsidy for Kerosene, LPG, and Petroleum[27], the Task Force on an IT Strategy for PDS[28], and the Task Force on an Aadhaar-enabled Unified Payment Infrastructure[29] have given a detailed roadmap for the implementation.

The e-KYC service can be deployed for linking existing beneficiary records with Aadhaar numbers based on the process outlined in Section 2.3. Examples include linkage of existing Ration Cards, pension accounts, scholarships, etc. with Aadhaar. This has the

[24] http://deity.gov.in/sites/upload_files/dit/files/DraftEDSBill_11042011.pdf
[25] http://indiabudget.nic.in/ub2012-13/bs/bs.pdf
[26] http://pmindia.gov.in/press-details.php?nodeid=1528
[27] http://finmin.nic.in/reports/Interim_report_Task_Force_DTS.pdf
[28] http://finmin.nic.in/reports/IT_Strategy_PDS.pdf
[29] http://finmin.nic.in/reports/Report_Task_Force_Aadhaar_PaymentInfra.pdf

twin benefit of achieving de-duplication and elimination of fakes and ghosts, while ensuring that the benefits reach the targeted beneficiaries.

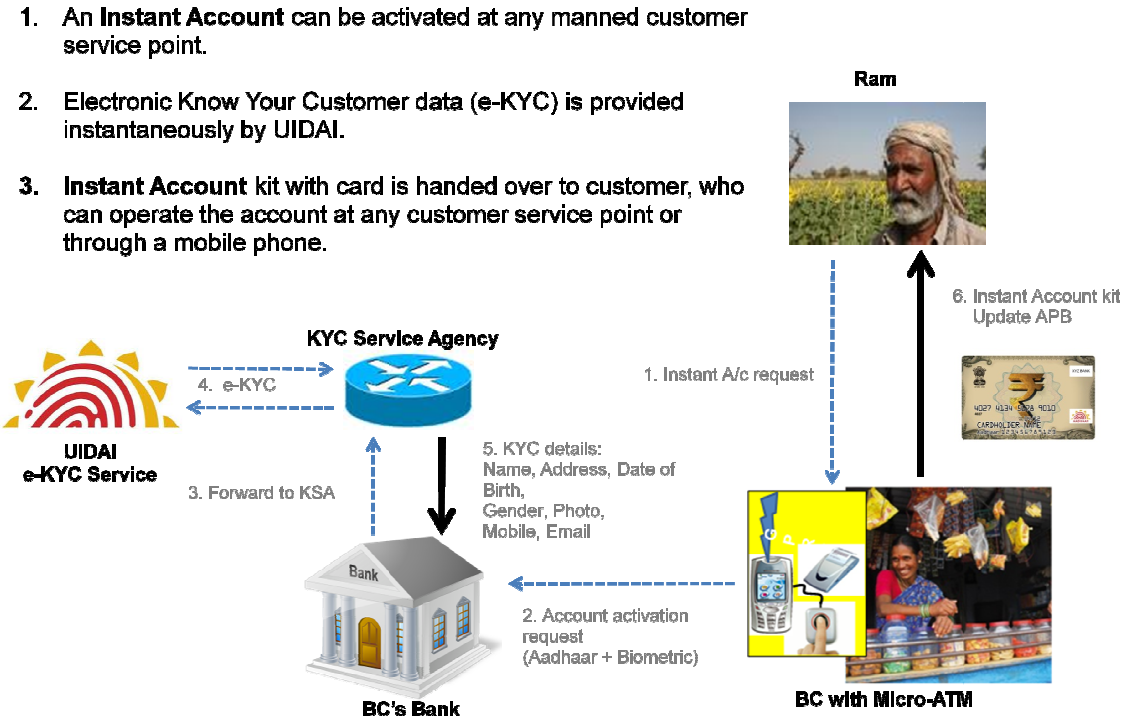
In cases where residents are applying for various Government-issued documents such as a Ration Card, Drivers' license, Caste certificate, Passport, Birth certificate, etc., the e-KYC service can be used for efficient service delivery, based on quick and accurate identification of the person.

4.1.2 Other applications

The e-KYC service can greatly reduce the KYC risk in the financial and telecom sectors.

The PMLA Rules, 2005 have been amended in 2010 vide Government of India, Gazette Notification GSR 980 (E) dated 16th December 2010. This amendment includes the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number in the list of officially valid documents. This has been followed by notifications from the sector regulators accepting Aadhaar as a valid KYC document. The Aadhaar e-KYC service is in full compliance with the provisions of the IT ct, 2000 and later amendments (Section 2.2).

Figure 2: Instant Account opening



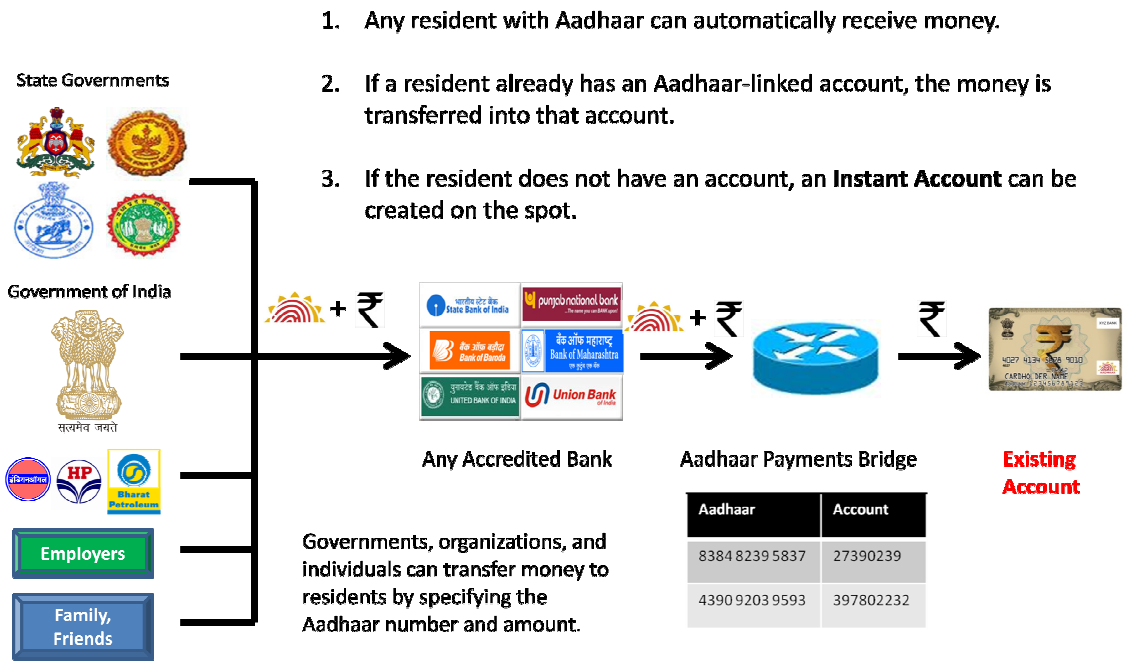
Banks can simplify the process of opening a bank account using the Aadhaar e-KYC service. Similarly, obtaining an insurance policy, purchasing capital market products such as mutual funds, and buying pension products, all can be greatly simplified through the use of the Aadhaar e-KYC service.

In the telecom industry, KYC has been an ongoing concern. The Department of Telecommunications has already notified Aadhaar as KYC for obtaining a mobile connection. A roadmap for the adoption of Aadhaar in the telecom sector is described in *Leveraging Aadhaar in the Telecom Sector*[30].

4.2 Aadhaar as a payment address

The Aadhaar number has the property of being a globally unique address for every resident of India, for life. This property makes it attractive to use Aadhaar as a payment address. The Aadhaar Payments Bridge has been recommended by the Task Force on an Aadhaar-enabled Payments Infrastructure, as a system that can route money to any resident on the basis of the Aadhaar number.

Figure 3: Aadhaar as a payment address



[30] http://uidai.gov.in/images/leveraging_aadhaar_telecom_sector_ver10_090412.pdf

With e-KYC, an Instant Account can be provided to anyone. The combination of Aadhaar as a Payment Address and e-KYC for an Instant Account can be used to create innovative products. For example, money can be sent to anyone with an Aadhaar number, irrespective of whether they have a bank account. If the receiver has an Aadhaar-enabled bank account, money can be transferred into it. If the receiver does not have an Aadhaar-enabled bank account, an Instant Account can be created on the basis of the Aadhaar number, with a debit freeze. Money transferred is credited into the Instant Account. The Instant Account can be activated during the first withdrawal on the basis of e-KYC.

5. Conclusion

The UIDAI is ready to offer the e-KYC service in a scalable, robust, and secure manner at scale. The Aadhaar e-KYC service can revolutionize service delivery in the public and private sector. It does not trade-off security for convenience and inclusion, and instead provides a solution that is secure, convenient, and inclusive.

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

KUA On-Boarding Process

Version 0.4

Release Date:

KYC User Agency (KUA) On-Boarding process is a reference document for UIDAI & KUAs involved in on-boarding process. This document provides detailed guidelines & steps for ensuring that the KUA's systems get aligned to UIDAI to begin e-KYC service delivery.

Table of Contents

KUA 1. DOCUMENT CONTROL 3

KUA1.1. Document Statistics 3
KUA1.2. Revision History 3
KUA1.3. How to Read this Document 3
KUA1.4. Legends 4

KUA 2. PROCESS OVERVIEW 5

KUA2.1. Objective 5
KUA2.2. Scope 5
KUA2.3. Prerequisites for Process 5
KUA2.4. Process Outcome 5
KUA2.5. Roles & Responsibilities 5

KUA 3. PROCESS DETAILS 7

KUA3.1. KUA On-Boarding Process 7
KUA 3.1.1. Process Description 8

KUA 4. ANNEXURE 11

KUA4.1. Forms, Templates & Checklist 11
KUA 4.1.1. KUA Request Form 11
KUA 4.1.2. Pre-production Approval template for KUA – UIDAI Business Team 12
KUA 4.1.3. Go – Live Notification 12
KUA4.2. Standards & Guidelines 12
KUA 4.2.1. e-KYC Policy Document 12

KUA 5. PROCESS CONTROLS 13

KUA5.1. Responsibility Matrix 13
KUA5.2. Control Check Points 13

KUA 1. Document Control

KUA1.1. Document Statistics

Type of Information	Document Data
Title	KUA On-Boarding Process
Document Revision #	0.3
Last Date Document was Updated	11/04/2013
Total Number of Pages	13
Document Filename	KUA Onboarding process Document_v0.3.docx
Document Owner	
Document Author(s)	Barkha Shah, Consultant
Document Change Reviewers	Rajesh Bansal, ADG-Finance Sudhir Narayana, ADG-Technology Center Tejpal Singh, ADG – Authentication Sameer Gupta, ADG – Authentication Deepti V Dutt – Senior Manager,PMU

KUA1.2. Revision History

Version No	Revision Date	Nature of Change	Initiated By	Date Approved	Date Released
0.1	03/03/13	First Draft	Barkha Shah		
0.2	08/03/13	Incorporated changes suggested by FI & Bangalore Tech Team over VC	Barkha Shah		
0.3	11/04/13	Changes are incorporated based on suggestion provided by Sanjith, Track Manager -UIDAI Tech Center	Barkha Shah		

KUA1.3. How to Read this Document

This process document is organised into below sections:

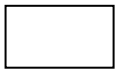
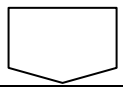
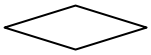
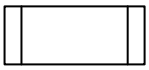
1. Process Overview
   a) **Goals and Objectives:** The section provides a description of what this process document intends to accomplish. The objectives represent specific measurable outcomes of this process document.
   b) **Scope:** This section lists the key activities covered in this process document.
   c) **Prerequisites for Process:** This section lists criteria that need to be fulfilled before the enrolment process covered in the scope of this document begins.

d) **Process Outcome**: This section informs what the output of the process is.

2. Process Details
   a) **Process Flowcharts:** Flowchart diagrams are used to define process in this document, showing the steps as boxes of various kinds, and their order by connecting these with arrows. This diagrammatic representation gives a step-by-step process flow. Process step is represented in these boxes, and arrows connecting them represent flow / direction of flow of data/information. Refer the Legends section to understand the significance of various symbols used in flowchart.
   b) **Process Description**: Process description is used for each flowchart to convey to the reader, a detailed description of each process step and references to annexure/other processes and sub processes. Refer Abbreviations used section for deciphering abbreviations used in the descriptions.

3. Annexure
   a) **Standards and Guidelines**: This section describes the standards recommended by UIDAI that need to be referred to during the enrolment process. Guidelines are provided to streamline the processes and help achieve better quality output.
   b) **Formats, Templates & Checklists:** This section consists of sample formats of various forms and checklists used in the scope of this process.

KUA1.4. Legends

	Signifies Start /End of Process
	Signifies Activity/Task
	Signifies an off page reference of a Sub Process
	Signifies a Decision Box
	Signifies Pre-Defined / External Process
	Signifies a Reference to either a Guideline(G), Form(F) or Control Check point (C) depending on the text used inside the circle

KUA 2. Process Overview

KUA2.1. Objective

The objective of this document is to provide detailed guidelines and activities on how to on-board various KYC User Agency (KUA). It also defines various technology interlock necessary between KUAs and UIDAI to carry out for e-KYC service delivery.

KUA2.2. Scope

KUAs are the entities currently acting as the Authorization User Agents (AUAs) and who are eligible to use e-KYC service in compliance with UIDAI's policies/procedures. Please note all KUAs are AUAs but converse is not true.

The existing AUA providers should explicitly register with UIDAI to enable them for providing e-KYC service to their customer base. The e-KYC service responds with resident demographic/photograph information to authorize the resident and uses the information to provide additional services.

The scope of this process is:

- To define the protocol for engagement between UIDAI and KUA
- Entering into the legal framework between KUA and UIDAI for carrying e-KYC service
- To define various inputs that are critical for success of process / activities

KUA2.3. Prerequisites for Process

- Existing or probable AUAs that would like to engage with UIDAI for e-KYC service delivery
- Need is expressed by probable/ existing AUAs for engagement as KUA.

KUA2.4. Process Outcome

- Signed Addendum (to be part of AUA agreement) between UIDAI and AUA
- Aligned Processes followed by KUA with UIDAI.

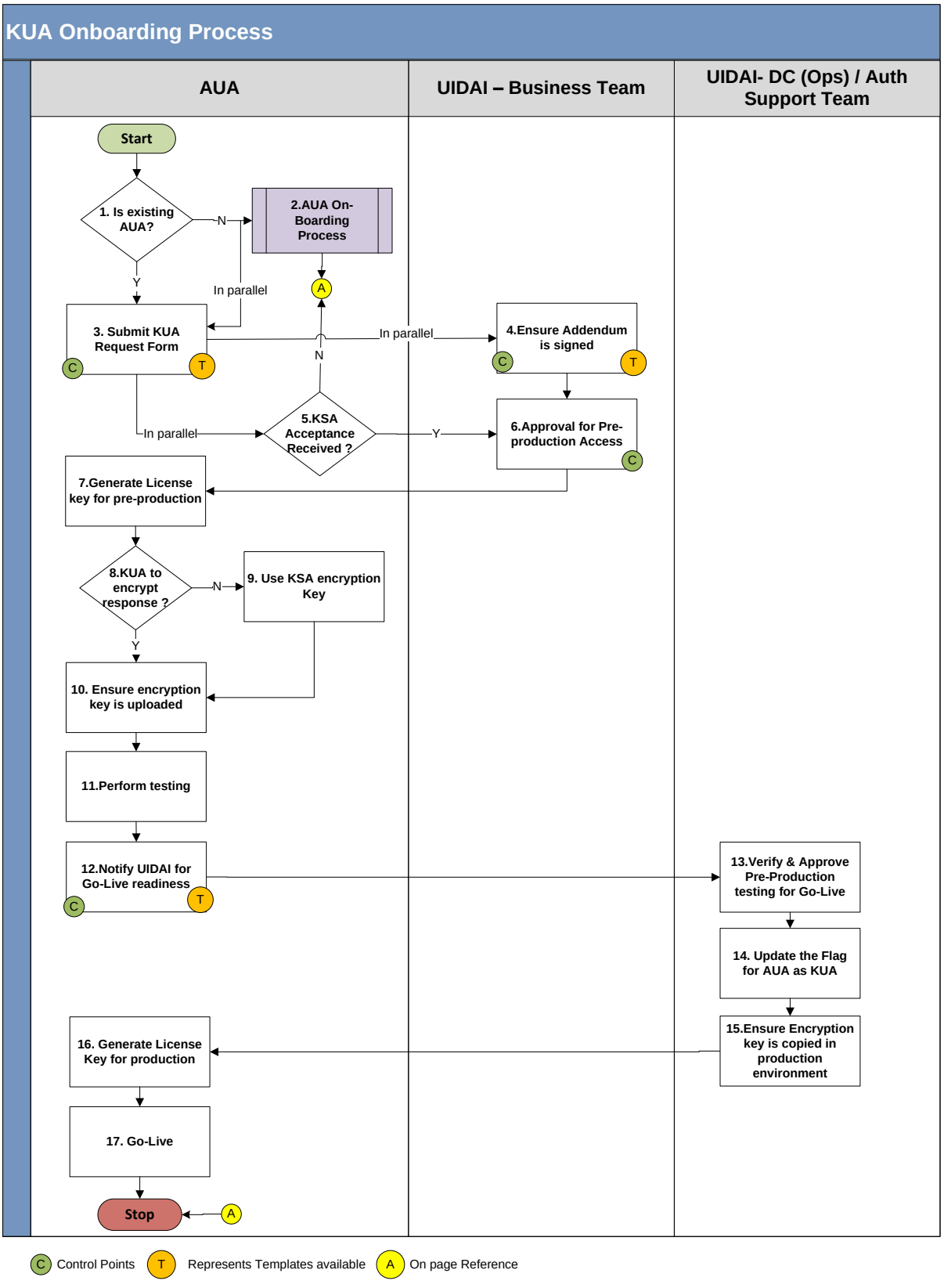
KUA2.5. Roles & Responsibilities

Role	Organization	Responsibilities
UIDAI Business Team	UIDAI	— Facilitate prospective KUAs to fill up and submit the Request form — Share all relevant knowledgebase documents for on-boarding process — Verify the Request form submitted by prospective KUA — Ensure all relevant internal approval from competent authority has been provided — Ensure AUA agreement is in place before Addendum is signed — Review & verify the Addendum and ensure it is signed between UIDAI & KUA — Track & resolve all open business issues faced by KUA during on-boarding process
DC (OPs)	UIDAI	— Validates the Go Live Checklist through logs or

Role	Organization	Responsibilities
Team	(or Auth Support team behalf of UIDAI)	perform testing from UIDAI side — Ensure all relevant internal approval from competent authority has been provided — Ensure License Key is obtained by KUA — Track & resolve all open technical issues faced by KUA during Pre-production & Production environment — Support in migration activity of KUA from Pre-production to Production environment.
KUA Nodal Person	KUA (AUA)	— Share contact & organization details with UIDAI — Ensure Business Plan & Technical Readiness plan is in place — Ensure Addendum is signed between UIDAI & KUA — Ensure proper arrangement is in place with KSA for end to end e-KYC service delivery — Submit & notify UIDAI about Go live Checklist — Ensure license key is available/obtained for Pre-production & Production environment — Ensure Encryption Key is uploaded — Set up required infrastructure of KUA readiness — Perform end to end testing in Pre-production — Ensure relevant test cases are available and reported for testing — Raise and track issues with concerned team during on-boarding process — Share credentials with UIDAI for seamless transaction during testing & Go Live — Adhere to contractual requirements & processes.
KSA Nodal Person	KSA	— Validate & confirms the KUA engagement with them for e-KYC service delivery — Support KUA on-boarding with respect to technical readiness — Share KSA credentials with KUA for seamless transaction during testing & Go Live — Extend KSA infrastructure required by KUA to carry out e-KYC transactions — Support KUA in Pre-production testing & production readiness.

KUA 3. Process Details

KUA3.1. KUA On-Boarding Process



KUA 3.1.1. Process Description

S.No	Steps	Responsibility	Reference
	START		
1	**Existing AUA?:** The process initiates with the decision whether the applicant is already the existing AUA with the UIDAI. If the applicant is already an existing AUA, then proceed to step 3. If the applicant is not yet engaged as AUA with UIDAI, then proceed to step 2.	Prospective KUA	
2	**AUA On-Boarding Process:** For cases if applicant is not engaged with UIDAI as AUA, then as per e-KYC Policy, the applicant has to first apply for AUA. Initiate the AUA On-Boarding Process to begin applicant's engagement with UIDAI as AUA. The detailed steps to be carried out by prospective AUA for on-boarding are covered in the AUA On-Boarding Process. It is recommended that in parallel prospective AUA shall also initiate the process for KUA by filling and submitting the KUA Request Form. Thus, this will facilitate the applicant to engage with UIDAI as AUA and at the same time it can also avail the e-KYC service as KUA. In parallel proceed to step 3.	Prospective KUA	External process- AUA On-Boarding Process
3	**Submit KUA Request Form:** The existing AUA can avail the e-KYC service by submitting the Request form for becoming KUA. It is recommended that in parallel prospective KUA shall also initiate the process of Addendum Signing (Step 4) and acceptance from KSA (Step 5)	Prospective KUA	Request Form (Refer section 4.1.1)
4	**Ensure Addendum Signing:** UIDAI business team will scrutinize the request form received from prospective KUA. The business team will take the requisite file approval from the competent authority. Post approval from the competent authority the request will be approved and UIDAI will sign the Addendum with prospective KUA. **Note:** The addendum shall be attached with existing AUA Contract.	UIDAI Business Team	Refer Addendum Copy
5	**Acceptance from KSA:** At the time of submission of Request Form prospective KUA has to select the preferred KSA that they would likely to engage with for e-KYC services. If KSA provides consensus for prospective KUA, proceed to step 6 'Approval for Pre-Production Access'. If KSA rejects prospective AUA application, proceed to	KUA	

S.No	Steps	Responsibility	Reference
	step 14, 'Stop'. **Note:** It shall be responsibility of KUA to ensure consensus from respective KSA has been obtained and informed/submitted to UIDAI.		
6	**Approval for Pre-Production Access:** UIDAI Business team will provide the approval for KUA to access the pre-production environment if following activities have been accomplished: i. Addendum has been signed between AUA & UIDAI. However, for case where applicant is not existing AUA, the Addendum shall be signed once the AUA agreement is in place. ii. Preferred KSA acceptance has received on engagement with prospective KUA.	UIDAI Business Team	Approval Template (Refer section 4.1.2)
7	**License Key Generation for Pre-Production Access:** On approval from UIDAI Business team, KUA shall generate the License key to access the Pre-Production environment. However, KUA can use the same AUA code for testing.	KUA	
8	**Encryption of Response XML:** If KUA decides to have response encrypted using their key then proceed to step 10,'Ensure License Key is Uploaded'. If response XML will be encrypted using KSA encryption key then proceed to step 9,'Use KSA Encryption Key'.	KUA	
9	**Use KSA Encryption key:** If KUA decides to use the KSA encryption key then UIDAI e-KYC Service shall encrypt using the KSA's public certificate. However, it is responsibility of KUA to ensure that encryption key has been uploaded by KSA and informed to UIDAI.		
10	**Ensure Encryption key is Uploaded:** The e-KYC response will be encrypted by the UIDAI using one of the following: i. If KUA has registered for its own digital certificate, UIDIA e-KYC service shall encrypt using KUA's public certificate. In this scenario KUA have to ensure that its encryption key is uploaded. ii. Otherwise, UIDAI e-KYC Service shall encrypt using the KSA's public certificate. In this scenario KUA must ensure that KSA encryption key is uploaded.	KUA	
11	**Perform Testing:** KUA along with engaged KSA performs end to end testing on UIDAI pre-production test bed. The timeline suggested for testing is 7-10 days (in addition to normal AUA on-boarding testing time). The testing will be carried out in following manner: - KUA will test the domain application by transmitting transaction request on pre-production environment. - KUA is expected to test the connectivity on KSA	KUA	

S.No	Steps	Responsibility	Reference
	testing environment as it is critical for integration testing of transmitting e-KYC request to UIDAI		
12	**Go Live Readiness Notification:** KUA notifies Business team, DC (OPs) team & KSA about its readiness for migration to production environment.	KUA	Go Live Notification Form (Refer section 4.1.3)
13	**Verify & Approval for Go-Live:** DC (OPs) team shall verify the transactions and other critical parameters based on logs or by performing testing at UIDAI side.	DC(OPs) / Auth Support Team	
14	**Update KUA Flag:** DC (OPs) team will update the flag for AUA and activate them as KUA to use e-KYC service.	DC(OPs) / Auth Support Team	
15	**Copy of Encryption Key:** DC(OPs) will ensure that encryption key (KUA or KSA as per the case) is copied from Pre-Production to Production environment	DC(OPs) / Auth Support Team	
16	**Generate License Key for Production:** Post approval from DC (OPs) team, KUA shall generate the License key for production environment. As a best practice, it is strongly recommended that AUA (KUA) should use the different license key to access KYC services with UIDAI. (*Though its technically feasible for AUA (KUA) to use the same authorization license key for e-KYC services.*)	KUA	
17	**Go Live:** Post migration & testing, KUA shall establishes production release and operation management mechanism. KUA Goes live and update status to UIDAI & KSA	KUA	
18	**STOP:** This process ends when the KUA systems are aligned to UIDAI terms & condition and is ready for e-KYC service delivery.		

KUA 4. Annexure

KUA4.1. Forms, Templates & Checklist

KUA 4.1.1. KUA Request Form

Organization Name:	<This shall be same as AUA details>
Address 1: Address 2: State: Pincode:	<This shall be same as AUA details>
Existing AUA Code*	
AUA Agreement Date*	Start Date: End Date:
Preferred KSA (Can select multiple KSAs)	Select your preferred / Engaged KSAs from existing KSA list
Proposed Business Scope w.r.t. e-KYC Service	
Management Point of Contact	
Nodal Person Name: Email-Id: Mobile No: Telephone No: FAX:	
Technical Point of Contact	
Nodal Person Name: Email-Id: Mobile No: Telephone No: FAX:	

** This information is relevant if applicant is already engaged as AUA with UIDAI. For entity that has not yet registered as AUA and applied for KUA, it is expected to process both the applications in parallel. However, the e-KYC service can be availed only if AUA application has been approved and is in Go Live stage.*

Submitted By *(from Applicant organization)*
Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Approved By *(from UIDAI)*
Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

KUA 4.1.2. Pre-production Approval template for KUA – UIDAI Business Team

Sr No	Activities	UIDAI – Business Team
1	Agreement signed between AUA & UIDAI	○ Yes Start date End Date ○ No
2	Addendum signed between KUA & UIDAI	○ Yes Start date End Date ○ No
3	File reference No for tracking physical file	

KUA 4.1.3. Go – Live Notification

Sr No	Activities	KUA	DC(OPs)
1	Encryption key is uploaded.	○ Yes ○ No	
2	KUA data logging for audit purposes provisioned.	○ Yes ○ No	
3	KUA has conducted end-to-end testing for 50 no of successful transactions in Pre-production environment.	○ Yes ○ No	
4	Resident consent process to obtain consent for every transaction is ready & deployed.	○ Yes ○ No	
Acceptance for Migration			○ Yes ○ No

KUA4.2. Standards & Guidelines

KUA 4.2.1. e-KYC Policy Document

For e-KYC Policy document refer link e-KYC Policy note.

KUA 5. Process Controls

KUA5.1. Responsibility Matrix

Activity	UIDAI Business Team (Authentication and Applications)	UIDAI DC (OPs)	KUA	KSA
Prospective KUA has submitted the Request Form	C,I		A,R	
Ensure that KUA applicant is already AUA with UIDAI	R	C	A	
Addendum signing between UIDAI & KUA	R	I	A,R	I
Consensus from preferred/selected ASA for authentication service delivery	I		A,R	R,C
Ensure Uploading of Encryption Key	I	C, R	A,R	R
Obtain license key for Pre-production & Production environment	I	C, R	A,R	I
Perform end to end testing in Pre-production & production environment	I	C, R	A,R	R
Submission of Go Live Notification to UIDAI	I	I	A,R	I
Validates the Go Live Checklist through logs or by performing testing at UIDAI side	C	A,R	C	
Updating KUA flag for concerned AUA	I	A,R	I	

KUA5.2. Control Check Points

Step	Document/Record	To be Maintained By
Submit KUA Request Form	- Request Form	UIDAI Business Team
Ensure Addendum Signing	- KUA & UIDAI Addendum template	UIDAI Business Team & KUA
Consensus / Acceptance of preferred / selected KSA	- Acceptance received through email or hard copy	UIDAI Business Team
Approval for Pre-Production Access	- Copy of signed AUA Agreement & Addendum	UIDAI Business Team
Submission of Go-Live Checklist	- Go-Live Notification Checklist	UIDAI
Updating KUA Flag	- Go Live Approval	DC(OPs) team

Unique Identification Authority of India

KYC User Agency Application Form

Organization Name: *(Same as AUA)*	
Address 1: Address 2: State: Pincode: *(Same as AUA)*	
Existing AUA Code*	
AUA Agreement Date*	Start Date: End Date:
Preferred KSA *(Can select multiple KSAs)*	
Proposed Business Scope w.r.t. e-KYC Service	
Management Point of Contact	
Nodal Person Name: Email-Id: Mobile No: Telephone No: FAX:	
Technical Point of Contact	
Nodal Person Name: Email-Id: Mobile No: Telephone No: FAX:	

** This information is relevant if applicant is already engaged as AUA with UIDAI. For entity that has not yet registered as AUA and applied for KUA, it is expected to process both the applications in parallel. However, the e-KYC service can be availed only if AUA application has been approved and is in Go Live stage.*

Submitted By *(from Applicant organization)*

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Approved By *(from UIDAI)*

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

KYC User Agency (KUA) Go Live Checklist

Unique Identification Authority of India

Go-Live Checklist*		
1	Encryption key is uploaded.	☐
2	KUA data logging for audit purposes provisioned.	☐
3	KUA has conducted end-to-end testing for 50 no of successful transactions in Pre-production environment.	☐
4	Resident consent process to obtain consent for every transaction is ready & deployed.	☐

*All the above items are mandatory and need to be completed before submitting for go live approval to UIDAI.

For additional information on the above e-KYC checklist items please refer UIDAI website http://uidai.gov.in

Please note that production KUA license key will be provided post UIDAI approval of this checklist.

KUA hereby confirms compliance to the current standards and specifications as published by UIDAI.

Submitted By *(from KUA organization)*

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Approved By *(from UIDAI)*

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

AADHAAR E-KYC

API SPECIFICATION - VERSION 2.0

MAY 2016

Table of Contents

1. INTRODUCTION 3

1.1 TARGET AUDIENCE AND PRE-REQUISITES 3
1.2 TERMINOLOGY 4
1.3 LEGAL FRAMEWORK 4
1.4 OBJECTIVE OF THIS DOCUMENT 4

2. UNDERSTANDING AADHAAR E-KYC SERVICE 5

2.1 AADHAAR AUTHENTICATION 5
2.2 ELIMINATING PHOTO COPIES AND COSTLY, INSECURE PAPERWORK 5
2.3 AADHAAR E-KYC API USAGE 6
2.4 CONCLUSION 6

3. AADHAAR E-KYC API 7

3.1 E-KYC API DATA FLOW 7
3.2 API PROTOCOL 8
3.2.1 *Element Details 8*
3.3 E-KYC API: INPUT DATA FORMAT 9
3.3.1 *Element Details 9*
3.4 E-KYC API: RESPONSE DATA FORMAT 11
3.4.1 *Element Details 12*

4. APPENDIX 16

4.1 RELATED PUBLICATIONS 16
4.2 CHANGES IN VERSION 2.0 FROM VERSION 1.0 16

1. Introduction

The Unique Identification Authority of India (UIDAI) has been established with the mandate of providing a Unique Identification Number (Aadhaar) to all residents of India. The UIDAI also provides the service of online authentication of identity on the basis of demographic and biometric data.

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a key requirement for access to financial products (payment products, bank accounts, insurance products, market products, etc.), SIM cards for mobile telephony, and access to various Central, State, and Local Government services. Today, customers provide physical PoI and PoA documents. Aadhaar is already a valid PoI and PoA document for various services in the Financial, Telecom, and Government domains. In addition, the UIDAI now also proposes to provide an e-KYC service, through which the KYC process can be performed electronically. As part of the e-KYC process, the resident authorizes UIDAI (through Aadhaar authentication) to provide their basic demographic data for PoI and PoA along with their photograph (digitally signed) to service providers.

Service providers can provide a paperless KYC experience by using e-KYC and avoid the cost of repeated KYC, the cost of paper handling and storage, and the risk of forged documents. Service providers may access the Aadhaar e-KYC service from UIDAI through the e-KYC API specified in this document.

1.1 Target Audience and Pre-Requisites

This is a technical document that is targeted at software professionals who are working in the technology domain, and are interested in incorporating the Aadhaar e-KYC API into their applications.

Readers must be fully familiar with following authentication documents published on UIDAI website (http://uidai.gov.in/auth) before reading this document.

1. Aadhaar Authentication Framework - http://uidai.gov.in/images/authDoc/d2_authentication_framework_v1.pdf
2. Aadhaar Authentication Operating Model - http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf
3. Aadhaar Authentication API Specifications - http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

In addition, readers are highly encouraged to read the following documents to understand the overall system:

1. UIDAI Strategy Overview - http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overview-001.pdf

2. The Demographic Data Standards and verification procedure Committee Report - http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
3. The Biometrics Standards Committee Report - http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf
4. Aadhaar Enabled Service Delivery - http://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf

1.2 Terminology

Readers are expected to be familiar with the general terminology used in Aadhaar authentication such as AUA, ASA, etc. before reading this section.

KYC User Agency (KUA): KUAs are AUAs that are eligible for the e-KYC service.

KYC Service Agency (KSA): KSAs are ASAs that are eligible to provide access to the e-KYC service through their network.

Note: All further references to AUA in the rest of this document automatically refer to KUA and similarly all references to ASA refer to KSA. Note that authentication AUA and sub-AUA automatically becomes KUA and their partner agencies in e-KYC. From a contract perspective, only KUA needs to have a contract with UIDAI.

IMPORTANT NOTE: All data sharing downstream from KSA to KUA to their partners must be done explicitly through "**informed resident consent**". KUAs shall not share the e-KYC response data with any other agency except for the purposes for which the e-KYC was done and with explicit consent of the resident for doing so. If KUA is engaging partners for conducting the e-KYC for their business transaction (Bank to their business correspondents for example) then KUA must have a contractual agreement such partners for e-KYC data protection and security. See KUA contract for full details.

1.3 Legal Framework

UIDAI has published necessary framework and processes around the Aadhaar e-KYC service. These documents specify KUA/KSA eligibility criteria, registration process, and the operating model.

1.4 Objective of this document

This document provides Aadhaar e-KYC API technical specifications. It contains details including API data format, protocol, and security specifications.

2. Understanding Aadhaar e-KYC service

This chapter describes Aadhaar e-KYC API, its background, and usage. Technical details related to the API are provided in subsequent chapters.

2.1 Aadhaar Authentication

Aadhaar authentication is the process wherein the Aadhaar Number, along with other attributes, including biometrics, are submitted online to the CIDR for its verification on the basis of information or data or documents available with it.

During the authentication transaction, the resident's record is first selected using the Aadhaar Number and then the demographic/biometric inputs are matched against the stored data which was provided by the resident during enrolment/update process. Alternatively, authentication can also be carried out on the basis of the OTP.

All biometric/OTP (single or multi-factor) authentication schemes are valid for e-KYC service too.

2.2 Eliminating Photo copies and Costly, Insecure Paperwork

Aadhaar is now a valid Proof of ID (PoI) and proof of Address (PoA) for most services is fast being the key document for banking, telco, insurance, Government subsidy programs, Passport, PAN card, etc. Considering the large number of Aadhaar holders in India and the ability to uniquely authenticate all Aadhaar holders, more and more services are accepting Aadhaar for their service delivery.

Traditionally all "Know Your Customer (KYC)" processes and verification of PoI and PoA are done using copies of PoI/PoA documents. It is commonplace to provide self-attested photocopies of these documents every time a bank account is opened, SIM card issued, insurance is purchased, etc.

Aadhaar e-KYC service eliminates the need for the resident to provide photo copy of Aadhaar letter and instead resident can simply authenticate and authorize UIDAI to share the Aadhaar letter data in electronic and secure (encrypted and digitally signed) fashion instead of leaving paper copies of the identity document everywhere.

Eliminating paper verification and storage removes fraud, fake document usage, paper storage cost, manual audit cost, etc. and makes entire process seamless, auditable, and secure. And most importantly this allows services such as bank account opening etc. done using a mobile handheld in rural environments without worrying about the authenticity of papers and trustworthiness of front end touch points.

2.3 Aadhaar e-KYC API Usage

The e-KYC API can be used (ONLY with the explicit authorization of the resident via Aadhaar biometric/OTP authentication) by an agency (KUA) to obtain electronic copy of Aadhaar letter. There are primarily two scenarios under which this API may be used:

1. **New customer/beneficiary**:
    a. In this case, KUA should use capture resident authentication data, invoke e-KYC API through a KSA network;
    b. Electronic copy of Aadhaar letter returned as part of the e-KYC API response is encrypted and digitally signed by UIDAI and can be used for electronic audit at a later stage; and
    c. This eliminates collecting photocopy of Aadhaar letter from resident. Using the electronic Aadhaar letter data obtained through this e-KYC API, the agency can create new customer account and service the customer.

2. **Existing customer/beneficiary**
    a. In this case, KUA should use capture resident authentication data, invoke e-KYC API through a KSA network;
    b. Electronic copy of Aadhaar letter returned as part of the e-KYC API response is encrypted and digitally signed by UIDAI and can be used for electronic audit at a later stage;
    c. Since the resident is already a customer/beneficiary, the agency can use a simple workflow to approve the Aadhaar linkage by comparing data retrieved through the e-KYC API against what is on record within UA database (in paper or electronic form); and
    d. Once verified, the existing customer/beneficiary record can be linked to the Aadhaar number and transaction trail can be stored for audit.

For both scenarios, the same e-KYC API is used to obtain the electronic version of Aadhaar letter data after successful resident authentication. Technical details for invoking the API are provided in subsequent chapters of this document.

2.4 Conclusion

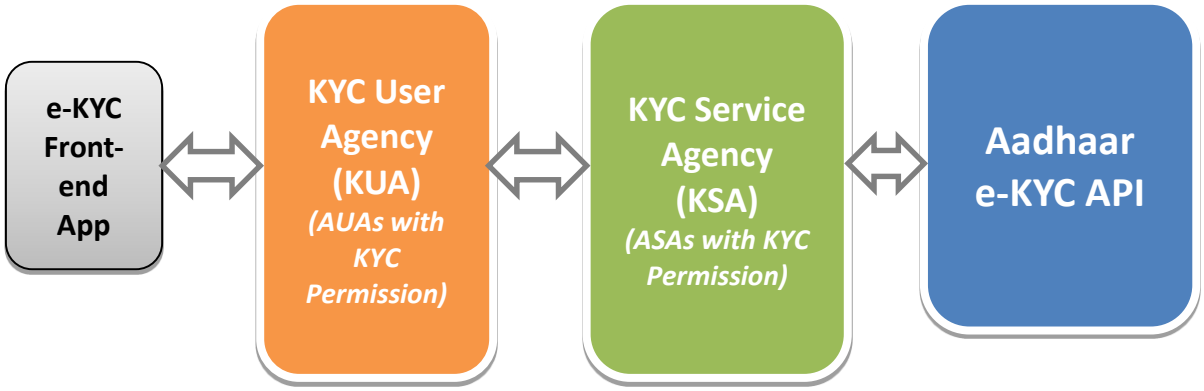
The Aadhaar e-KYC API provides a convenient mechanism for agencies to offer an electronic, paper-less KYC experience to Aadhaar holders eliminating insecure and costly paper process that exist today. The e-KYC service provides simplicity to the resident, while providing cost-savings from managing and processing paper documents to the KUA.

3. Aadhaar e-KYC API

This chapter describes the API in detail including the flow, communication protocol, and data formats.

3.1 e-KYC API Data Flow

Following the data flow of a typical e-KYC API call from left to right and back.



1. e-KYC front-end application captures Aadhaar number + biometric/OTP of resident and forms the encrypted PID block (see Authentication API for details)
2. KUA forms the Auth XML using the PID block, signs it, uses that to form final e-KYC input XML and sends to KSA (if this is delegated to KSA, KSA also could do the input XML creation and signing)
3. KSA forwards the KYC XML to Aadhaar e-KYC service
4. Aadhaar KYC service authenticates the resident and if successful responds with digitally signed and encrypted XML containing resident's latest demographic and photograph information
5. E-KYC response (containing demographic data and photograph), by default, is encrypted with KUA public key
    - If KUA key is NOT available within CIDR, KSA public key will be used provided KSA is approved to do so.
    - If "de" attribute is used in input XML to delegate decryption to KSA (this can be done at transaction level), then KSA key will be used to encrypt response, provided KSA is approved to do so (this option allows KUAs to dynamically delegate decryption to KSA based on their relationship and setup with KSA)
6. KSA sends the response back to KUA enabling paperless electronic KYC. KUA should keep the digitally signed XML as-is (equivalent to physical Aadhaar letter) for audit purposes.

Note: Digital signature in input (KUA or KSA) is independent of response data encryption. Input signature is used by UIDAI server to assert authenticity of the requesting agency whereas response encryption is to protect resident data.

3.2 API Protocol

Aadhaar e-KYC service is exposed as stateless service over HTTPS. Usage of open data format in XML and widely used protocol such as HTTP allows easy adoption by the user agencies. To support strong end to end security and avoid request tampering and man-in-the-middle attacks, it is essential that encryption of input PID data happens at the time of capture on the capture device.

Following is the URL format for Aadhaar e-KYC service:

```
https://<host>/kyc/<ver>/<ac>/<uid[0]>/<uid[1]>/<asalk>
```

API input data should be sent to this URL as XML document using Content-Type "application/xml" or "text/xml".

For security reason PID data collected for Aadhaar e-KYC must NOT be stored on any device or server. It's essential for KSA and KUA to maintain audit records for all the authentication request metadata along with the response and protect the PII data.

3.2.1 Element Details

host – Aadhaar e-KYC API server address. Actual production server address will be provided to KSAs. Note that production servers can only be accessed through secure leased lines. KSA server should ensure that actual URL is configurable.

Next part of the URL "kyc" indicates that this is e-KYC API call. Ensure that this is provided.

ver – e-KYC API version (optional). If not provided, URL points to current version. UIDAI may host multiple versions for supporting gradual migration. As of this specification, default production version is "**2.0**".

ac – A unique code for the AUA (KUA and AUA codes are same since KUA is an AUA having access privilege to e-KYC service) which is assigned by UIDAI. This is an alpha-numeric string having maximum length 10.

uid[0] and **uid[1]** – First 2 digits of Aadhaar Number. Used for load-balancing.

asalk – A valid ASA license key. ASAs must send one of their valid license keys at the end of the URL. It is important that license keys are maintained safely. **When adding license key to the URL, ensure it is "URL encoded" to handle special characters**.

For all valid responses, HTTP response code 200 is used. All application error codes are encapsulated in response XML element. In the case of connection and other server errors,

standard HTTP error response codes are used (4xx codes such as 403, 404, etc.). HTTP automatic redirects also should be handled by ASA server.

ASA server must send one of their valid license keys as part of the URL (see details above). E-KYC API is enabled only for valid KSAs and only for their registered static IP addresses coming through a secure private network.

3.3 e-KYC API: Input Data Format

Aadhaar KYC API uses XML as the data format for input and output. To avoid sending unnecessary data, do not pass any optional attribute or element unless its value is different from default value. Any bad data or extra data will be rejected.

Following is the XML data format for authentication API:

```
<Kyc ver="" ts="" ra="" rc="" mec="" lr="" de="" pfr="">
  <Rad>base64 encoded fully valid Auth XML for resident</Rad>
</Kyc>
```

3.3.1 Element Details

Element: **Kyc** (mandatory)
Root element of the input XML for e-KYC API

Attributes:

- **ver** – (mandatory) version of the KYC API. Currently only valid value is "2.0".
- **ts** – (mandatory) Timestamp at the time of capture of authentication input. **This value must match** "ts" attribute of "PID" block of the resident authentication packet under "Rad" element.
    - **If this value is not matching with PID ts, then, an error will be generated**.
    - Front-end application on the device must send the PID "ts" value to KUA server to ensure PID capture timestamp is used "as-is" within this XML. This is to ensure authentication input cannot be independently used for e-KYC later.
- **ra** – (mandatory) Resident authentication type. Valid values are "F", "I", "O", "P" or any combination of these. Front end e-KYC application that capture the resident authentication PID block, should determine value of this attribute based on what is captured. For example, if resident authentication uses fingerprints, then this should be "F", if both fingerprint and OTP are used this should be "FO", and so on (see table below for all values). This and actual authentication factors within PID block do not match, an error is returned.
- **rc** – (mandatory) Represents resident's explicit consent for accessing the resident's identity and address data from Aadhaar system. Only valid value is "Y". Without explicit consent of the Aadhaar holder application should not call this API.

- **mec** – (optional) Represents resident's explicit consent for accessing the mobile number and email address of the resident from Aadhaar system. Valid values are "Y" and "N". Default value is "N" (by default, this API does not return mobile and email data).
- **lr** - (optional) Flag indicating if AUA application require local language data in addition to English. Valid values are "Y" and "N". Default value is "N" (by default, this API does not return local Indian language data).
- **de** – (optional) Flag indicating if KUA is delegating decryption to KSA. If this flag is set to "Y", then KSA public key will be used to encrypt e-KYC response XML instead of KUA key provided KSA is allowed to do so.
    - **This is OPTIONAL attribute and hence should be used ONLY when KUA requires to change the default option based on KSA setup. <u>This option works only if KSA is approved to do decryption</u>**.
    - By default, KUA public key is always used to encrypt e-KYC response.
    - If KUA key is NOT available in CIDR, KSA key will be used to encrypt provided KSA is authorized to do so.
    - A dynamic option of setting "de" attribute to "Y" allows KUA to make this choice at transaction level based on the KSA they use for e-KYC service.
- **pfr** – (optional) Print format request flag for retrieving E-Aadhaar document in PDF and XML format as part of response . Only valid values are `"Y"` and `"N"`. If `"Y"` is passed the print format is returned in the response in addition to XML. Applications are highly encouraged to use XML data to avoid manual verification or paper printing.

e-KYC front-end application **must ensure it takes an "explicit informed resident consent"** authorizing the KUA to retrieve the resident data. E-KYC Application should not hard-code values for "rc" and "mec" under any circumstances and should ensure that both consents are taken explicitly through the application UI.

Element: **Rad** (mandatory)

This element contains base64 encoded Auth XML for resident. Authentication input XML must be fully compliant to Aadhaar Authentication API specification.

It is important to note that resident authentication XML (provided under "Rad" element) MUST have its "txn" attribute value starting with **"UKC:"** as the namespace for KYC API. Otherwise, this API will throw appropriate error indicating that the transaction value is invalid.

Any valid Authentication API version and features can be used while invoking e-KYC. Only restriction being that the prefix of "txn" attribute value of the authentication input XML (authentication namespace) must start with **"UKC:"**.

IMPORTANT NOTE*:* **Digital Signature at e-KYC XML level is optional**

- The e-KYC request XML may be digitally signed for message integrity and non-repudiation purposes.

3.4 e-KYC API: Response Data Format

Resident data as part of the response based on successful authentication (thus resident authorizing UDIAI to share his/her data with the KUA/KSA) is fully encrypted using KUA public key (or KSA public key if KUA delegates it to KSA).

Response XML for the KYC API is as follows:

```
<Resp status="" ko="" ret="" code="" txn="" ts="" err="">encrypted and
base64 encoded KycRes element</Resp>
```

Element:

- **Resp** - container for keeping encrypted e-KYC response. Value of the "Resp" element is base64 encoded version of the encrypted "KycRes" element (see "KycRes" element description later).

Attributes:

- **status** - Indicates high level status of the API call. It can have values "0" or "-1". If the status is "0", it means that the encrypted data contained within the "Resp" element is valid. If it contains "-1", it means the data should not be decrypted and used.
- **ko** – This attribute contains either value "KUA" or "KSA" or "". If response is encrypted with KUA key, this will have value "KUA", otherwise, if it is encrypted with KSA key, this will have value "KSA". If there were any errors (when "status" is "-1"), this attribute will have blank value.
- **ret, code, txn, ts, err** – These attributes are exactly same as what is inside the encrypted block. See "KycRes" element and its attribute descriptions below. **These attributes are also made available at this element for KSA to have audit capability even when the actual response is encrypted with KUA key**.

Note: As explained before, "KycRes" element is encrypted using the following logic:

1. By default, KUA public key is used to encrypt response data
2. If "de" attribute in input XML is set to "Y" or if KUA public key is not available in CIDR, KSA public key is used to encrypt, provided KSA is approved to do so.
3. If neither KUA nor KSA public keys are available in CIDR, an error is generated.

Once decoded and decrypted, "KycRes" has the following structure:

```
<KycRes ret="" code="" txn="" ts="" ttl="" actn="" err="">
  <Rar>base64 encoded fully valid Auth response XML for resident</Rar>
  <UidData uid="">
    <Poi name="" dob="" gender="" phone="" email=""/>
    <Poa co="" house="" street="" lm="" loc="" vtc=""
         subdist="" dist="" state="" country="" pc="" po=""/>
    <LData lang="" name="" co="" house="" street="" lm="" loc="" vtc=""
         subdist="" dist="" state="" country="" pc="" po=""/>
    <Pht>base64 encoded JPEG photo of the resident</Pht>
    <Prn type="pdf">base64 encoded signed Aadhaar letter for printing</Prn>
  </UidData>
  <Signature/>
</KycRes>
```

3.4.1 Element Details

Element: **KycRes**

Attributes:

- **ret** – this is the main KYC API response. It is either "y" or "n".
- **code** – unique alphanumeric response code for e-KYC API having maximum length 40. AUA is expected to store this for future reference for handling any disputes. Aadhaar KYC server will retain e-KYC trail only for a short period of time as per UIDAI policy.
- **txn** – e-KYC API transaction identifier. This is exactly the same value that is sent within the request XML.
- **ts** – Timestamp when the response is generated. This is of type XSD dateTime.
- **ttl** – "*Time To Live*" for demographic data within AUA system. AUAs may not use the resident data obtained through this API beyond this time and should use this API to obtain latest resident data.
    - It is important to understand that demographic information changes from time to time (address change, mobile number change, etc.).
    - AUAs should build applications understanding the nature of this data and ensure that they use this API from time to time to obtain latest KYC data of the resident.
- **actn** – (optional). This attribute may or may not exist in response. This attribute will have specific action codes (published from time to time) meant for future purposes to be shown to resident/operator.
    - **This attribute MUST be sent to front-end application by KSA and KUA to ensure action and corresponding message is displayed to resident/operator**.
- **err** – Failure error code. If e-KYC API fails ("ret" attribute value is "n"), this attribute provides any of the following codes (for latest updates on error codes, see https://developer.uidai.gov.in/site/api_err):
    - **"K-100"** – Resident authentication failed
    - **"K-200"** – Resident data currently not available
    - **"K-540"** – Invalid KYC XML

- **"K-541"** – Invalid e-KYC API version
- **"K-542"** – Invalid resident consent ("rc" attribute in "Kyc" element)
- **"K-543"** – Invalid timestamp ("ts" attribute in "Kyc" element)
- **"K-544"** – Invalid resident auth type ("ra" attribute in "Kyc" element does not match what is in PID block)
- **"K-545"** – Resident has opted-out of this service. This feature is not implemented currently.
- **"K**-546" – Invalid value for "pfr" attribute
- **"K-550"**- Invalid Uses Attribute
- **"K-551"** – Invalid "Txn" namespace
- "**K-552**" = Invalid License key
- **"K-569"** – Digital signature verification failed for e-KYC XML
- **"K-570"** – Invalid key info in digital signature for e-KYC XML (it is either expired, or does not belong to the AUA or is not created by a well-known Certification Authority)
- **"K-600"** – AUA is invalid or not an authorized KUA
- **"K-601"** – ASA is invalid or not an authorized KSA
- **"K-602"** – KUA encryption key not available
- **"K-603"** – KSA encryption key not available
- "**K-604**" – KSA Signature not allowed
- **"K-605"** – Neither KUA key nor KSA encryption key are available
- "**K-955**" – Technical Failure
- **"K-999"** – Unknown error

Element: **Rar**

This element contains base64 encoded version of the entire authentication API response XML (AuthRes element – see Authentication API specification document) for the resident authentication.

Element: **UidData**

This element and its sub-elements contain demographic data and photograph of the resident as per Aadhaar system.

Attributes:

- **uid** – 12-digit Aadhaar number of the resident

Element: **Poi**

This element contains resident's name within Aadhaar system.

Attributes:

- **name** – Name of the resident
- **dob** – Date of birth of the resident in DD-MM-YYYY format
- **gender** – Gender of the resident. Valid values are M (male), F (female), and T (transgender)

- **phone** – Mobile phone if any based on "mec" attribute
- **email** – Email address if any based on "mec" attribute

Element: **Poa**

This element contains resident's address within Aadhaar system.

Attributes:

- **co** – "Care of" person's name if any
- **house** – House identifier if any
- **street** – Street name if any
- **lm** – Landmark if any
- **loc** – Locality if any
- **vtc** – Name of village or town or city
- **subdist** – Sub-District name
- **dist** – District name
- **state** – State name
- **country** – Country name
- **pc** – Postal pin code
- **po** – Post Office name if any

Element: **LData**

This element contains resident's name and address in local Indian language which was used while last data update. This is returned only if "lr" attribute in the API input XML is set to "Y".

Attributes (all data in Indian local language):

- **lang** – Local language code (see table below)
- **name** – Name of the resident
- **co** – "Care of" person's name if any
- **house** – House identifier if any
- **street** – Street name if any
- **lm** – Landmark if any
- **loc** – Locality if any
- **vtc** – Name of village or town or city
- **subdist** – Sub-District name
- **dist** – District name
- **state** – State name
- **country** – Country name
- **pc** – Postal pin code
- **po** – Post Office name if any

Language	Language code
Assamese	01
Bengali	02
Gujarati	05
Hindi	06
Kannada	07
Malayalam	11
Manipuri	12
Marathi	13
Oriya	15
Punjabi	16
Tamil	20
Telugu	21
Urdu	22

Element: **Pht**

This element contains base64 encoded JPEG photo of the resident.

Element: **Prn**

This element contains base64 encoded e-Aadhaar PDF of the resident that is digitally signed. This is useful for applications where a paper print is still needed. Application providers are highly encouraged to move away from the paper printing and instead store and use the digitally signed XML data which is part of the response.

Element: **Signature**

This is the root element of UIDAI's digital signature. This signature can be verified using UIDAI public key. Signature complies with W3C XML signature scheme.

For more details, refer: http://www.w3.org/TR/xmldsig-core/

4. Appendix

4.1 Related Publications

Demographic Data Standards	http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
Aadhaar Authentication API Specification	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf
XML Signature	http://www.w3.org/TR/xmldsig-core/

4.2 Changes in Version 2.0 from Version 1.0

New (2.0)
eKYC response optionally provides print format in additional to xml. This option is enabled via “pfr” in the request
Country is added in address in eKYC response
Additional error codes added

Aadhaar

Authentication
Standards and Specifications

Version 1.7

May 2012

Unique Identification Authority of India

Sl.No	Name of the Standards and Specifications Document	Link/ Reference to the Document
1.	Aadhaar Authentication API Specification 1.6	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf
2.	Aadhaar Best Finger Detection API Specification 1.6	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf
3.	Aadhaar OTP Request API Specification 1.5	http://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf
4.	Biometric Devices Specifications for Aadhaar Authentication	http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf
5.	Demographic Data Standards	http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
6.	Biometric Data Interchange Standards	ISO/IEC 19794-2:2005, ISO/IEC 19794-4:2005
7.	Date and Time format Standard	ISO_8601
8.	XML Signature	http://www.w3.org/TR/xmldsig-core/
9.	Basic checks to be performed by ASA before forwarding an authentication packet to CIDR	ASA should check structural validity of the AUA packet (against XSD) and checks signature of the AUA to ensure no unwanted, malicious requests are sent through.
10.	Audit logging requirements	Authentication audit trail should be for a minimum of 6 months Auditable fields - API Name, AUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-PII data.

11.	Security Policy & Framework for UIDAI Authentication 1.0	http://uidai.gov.in/images/authDoc/d3_4_security_policy_framework_v1.pdf

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

Creating a Circle of Trust

Aadhaar Authentication Services

A Strategy Paper

Contents

1 Background 3
2 Aadhaar Authentication 3
3 Benefits of Aadhaar Authentication 4
4 Authentication Ecosystem 5
5 Technology Architecture 5
6 Authentication Framework 7
7 Legal & Contractual Framework 8
8 Charging Policy 8
9 Risks 9
10 Enabling Adoption of Aadhaar Authentication 9
11 Conclusion 10
12 Glossary 11

1 Background

Identity and authentication systems based on biometrics have long existed in the country & elsewhere in the world. As early as 1858, William James Herschel, an employee of the East India Company, wanted a good way to seal a contract with a Bengali firm, and settled on using a handprint on the contract. Two years later, Herschel became a magistrate at Nuddea. One of his official duties was to make sure that not only did the locals of the area receive the pensions that were due them, but to prevent as much fraud as possible. High illiteracy rates, and therefore the inability to get a signature, drastically raised the potential for fraud. Remembering the success of the handprint, Herschel began requiring pensioners to use their fingerprint as a form of signature in order to receive the money due them.

Over the years, what started as an empowering tool became a symbol of illiteracy, helplessness and surrender of the weak to the powerful. Aadhaar Authentication services proposes to restore use of biometrics to its rightful place – as a powerful tool that will help the poor and marginalised assert their right to seek services on equal terms as the urban non-poor. By combining technology and biometrics, Aadhaar authentication service proposes to remove current authentication barriers faced by the marginalized in accessing services. Biometric based authentication would be offered alongside existing authentication mechanisms such as PINs and passwords.

The Unique Identification Authority of India (UIDAI) has been created, with the mandate of providing a Unique Identity (Aadhaar) to all Indian residents. The identity infrastructure in India today is a patchwork of multiple documents that are used as proof of identity – different documents demanded by different agencies first to establish entitlement to a service and then repeatedly every time that the resident has to avail of his entitlement. This will be replaced by Aadhaar, a **nationally valid unique life time identifier** that has the potential of transforming identity verification in India in ways that are currently beyond our vision.

This strategy paper outlines the core aspects of Aadhaar Authentication Service.

2 Aadhaar Authentication

The UIDAI will provide online authentication using demographic and biometric data. The Unique Identification (Aadhaar) Number, which uniquely identifies residents, will give individuals the means to clearly establish their identity to public and private agencies across the country.

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (including biometrics) is submitted to the Central Identities Data Repository 'CIDR' for its verification and such repository verifies the correctness thereof on the basis of information or data available with it. Aadhaar authentication service only responds with a "yes/no" and no personal identity information is returned as part of the response.

The purpose of Authentication is to enable residents to prove identity and for service providers to confirm that the resident is 'who they claim to be' in order to supply services and give access to benefits.

Aadhaar authentication will provide several ways in which residents can authenticate themselves using the system. Authentication can be 'Demographic Authentication' and/or 'Biometric Authentication'. But, in all forms of authentication the Aadhaar Number needs to be submitted so that this operation is reduced to a 1:1 match.

Aadhaar authentication is an online authentication service which will have certain distinct advantages over offline authentication in terms of being more cost effective, more secure and allowing portability.

3 Benefits of Aadhaar Authentication

The adoption of authentication services provided by UIDAI can help deliver following benefits:

A. Establishing Identity:
- Adding new beneficiaries – Various service delivery organizations can authenticate residents against CIDR and add them to their programs. Aadhaar-based authentication would not only bring such residents into folds of basic social welfare programs such as PDS & RSBY, but also allow them access to social levellers such as banking & telecom which have so far been denied to them for want of identity proof.
- Confirming Beneficiary – Various social sector programs, where beneficiaries need to be confirmed before delivery of the service can use Aadhaar authentication. This will not only help curb leakages but also ensure that the targeted beneficiary is not denied entitlement.
- Attendance tracking – Programs such as SSA and NREGA where outlay/wages is linked to beneficiary attendance can use Aadhaar authentication for attendance tracking.
- Financial transactions – One of the biggest benefits of Aadhaar-based authentication is expected to be in financial inclusion segment. Micro-ATM devices on Aadhaar-based authentication have the potential of changing financial landscape of the country.
- Move service delivery towards a demand-driven, portable, beneficiary led system – Since beneficiaries can authenticate their Aadhaar anywhere, various service delivery processes can be re-engineered to make delivery more flexible & favourable to the beneficiaries.
- Access to relevant MIS and empowerment of beneficiary – Aadhaar can be used to empower beneficiaries and provide self-help facilities for activities such as checking their entitlements, services delivery timeline, log grievances etc. The same can be enabled through self-service kiosks, mobile phones, call centres etc.

B. Improving Efficiency & Transparency in Service Delivery
- Track end-to-end service delivery process – Aadhaar authentication if implemented across the service delivery process / supply chain will help curb leakages and diversions, and help identify bottlenecks in delivery.
- Accountability / vigilance – Besides tracking beneficiaries, Aadhaar-based authentication can also be used for authenticating officials / members responsible for audits, vigilance etc. Such usage is expected to bring in more accountability & transparency in the social sector programs.
- Access control: Aadhaar authentication could be used to control access/entry to restricted areas such as airports, hotels, examination halls etc.

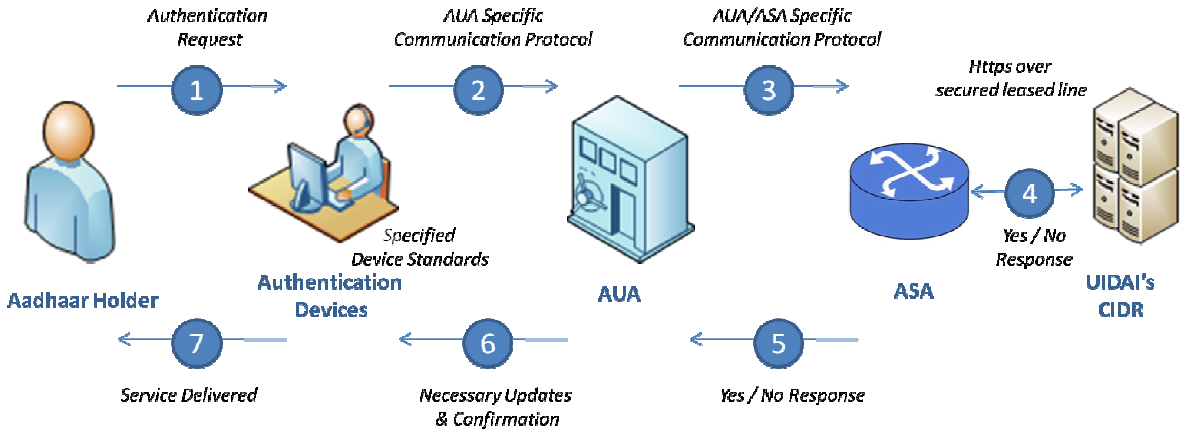
C. Address and Demographic Verification:
- Address verification: Address verification, which is a key requirement for providing some of the services like telephone connection, banking products, could be done through Aadhaar-based authentication. This is expected to substantially reduce the cost of KYC in providing these services & at the same time provide a reliable verification mechanism.
- Demographic data verification: Demographic data like age and gender can be verified through Aadhaar authentication.

4 Authentication Ecosystem

Authentication service will require involvement of various ecosystem members. Various members who are expected to play a role in Aadhaar authentication ecosystem include:

- Aadhaar Holders/ Residents – Residents who have already been issued Aadhaar number.
- Terminals / Merchants – Terminals are devices deployed by AUAs to provide services to residents. These devices will host applications of the AUA and initiate residents' authentication requests. Merchants are the outlets that provide the service at grass-root level & maintain the terminals.
- Authentication User Agencies (AUAs) – An organization or an entity using Aadhaar authentication as part of its service delivery cycle
- Authentication Service Agencies (ASAs) – An entity that transmits authentication requests to the MSP on behalf of self or one or more AUAs
- Managed Service Provider (MSP) – An organization appointed by UIDAI that manages UIDAI's CIDR
- Authentication Service Providers (AuSP) – Entities proposed to be created that will provide CIDR based authentication services to various authentication user agencies
- UIDAI's CIDR – A centralised database in one or more locations containing all Aadhaar numbers issued along with the corresponding demographic and biometric information
- Network / Connectivity Provider – Entities that would provide required connectivity between other members of authentication ecosystem – between merchant and AUA, between AUA and AuSP/MSP, between AuSP/MSP and CIDR
- Device Suppliers – Organizations that would manufacture, supply and maintain devices required for carrying out authentication

The relationship between various players can be depicted as:



5 Technology Architecture

The fundamental principles that will guide the technology architecture include:

1. High volume light weight ubiquitous on-line services – When Aadhaar authentication gains traction, the expected volume of per day authentication transactions is to the tune of 10 million. To ensure that not only CIDR but also the country's network is able to support such volume, the authentication transactions would be very light weight. Since authentication requests will origin from every nook & corner of the country, AUAs

would be able send authentication requests over any form of connectivity available including mobile telecom, broadband, PSTN etc.

CIDR would be responding to authentication requests instantly. The entire cycle time of AUA transmitting authentication request to CIDR and getting a response in return is expected to be within 5-8 seconds.

2. High performance large scale distributed computing application architecture – Supporting the expected volume, geographical spread & response time requires not only the authentication requests to be light weight, but also back end capabilities. Some principles that could be deployed to ensure high performance large scale support include distributed computing, multiple Authentication Service Providers (AuSPs) etc.

3. Supporting and guiding rich client software to be deployed on large number of hardware in remote locations – Rich client software would be required for capturing Aadhaar authentication request as well as specific requirements of the AUA. For example, a PDS client would record details of food grains to be drawn in addition to authentication attributes. AUAs may also require additional features such as multilingual and voice support. To ensure consistent processing of authentication requests originating from different AUAs, UIDAI will provide a common API that the AUAs can use for developing their authentication clients. UIDAI will also publish device specifications for carrying out different types of authentication requests.

4. Fraud detection architecture and development of fraud rules for Aadhaar authentication services – UIDAI will deploy a robust fraud management system to detect potential system abuses. UIDAI will develop fraud detection rules and will regularly review & update the same. In addition, the authentication transaction logs of an individual will be maintained to resolve frauds/disputes if any.

5. Designing portal for monitoring and reporting on Aadhaar authentication services – Aadhaar authentication service will be rolled out through a web portal through which various key ecosystem members can self manage their information and requirements. Some potential uses envisaged include AUA registration, device registration, Residents' ability to view their transaction logs etc.

6. Data security and integrity for transfer of data from field location – Adequate measures will be taken to protect Aadhaar authentication infrastructure against attacks or misuse. Strong encryption methods, use of open and established security standards, assessment of threats and vulnerabilities, and presence of auditable security controls, processes, and enforcement mechanisms etc. will be adopted to ensure security and integrity of data transfer from field to CIDR. The objective will be to detect and prevent intrusions, corruption, and disruption to the maximum extent possible.

6 Authentication Framework

Authentication is essentially an assurance that the resident is 'who they say they are'. UIDAI would be developing an authentication framework based on following concepts:

- Authentication environment – UIDAI will provide authentication in various types of environment such as public/non-trusted, trusted and trusted-cum-operator authenticated.
- Authentication attributes – UIDAI will support biometric (finger print & iris) as well as non-biometric (such as OTP, PIN, DoB/Age, mobile number etc.) attributes for authentication.
- Authentication factors – UIDAI will support multiple authentication factors:
  - What you extrinsically have (ownership factor): Attributes that the user uniquely owns and is *replaceable* (e.g., a card, security token or cell phone) UIDAI will support OTP received on registered mobile phone as the ownership factor
  - What you know (knowledge factor): Attributes that the user individually knows as a secret (e.g., a password or personal identification number (PIN)) UIDAI will support PIN as knowledge factor
  - What you intrinsically have (inherence factor): Attributes that the user is uniquely born with and is *irreplaceable* (e.g., fingerprint, iris pattern) UIDAI will support fingerprint & iris pattern as inherence factors

  Every authentication factor has its own advantages, limitations and challenges; there would be certain segments of residents who may not be able to authenticate themselves using a particular attribute. For example, some limitations of biometric authentication are false accepts & false rejects, inability to authenticate people with no fingers / iris etc. Similarly, challenges of OTP based authentication include penetration of mobile phones in the country, potential of misplacing / loosing mobile phones, illiteracy levels etc.

An authentication factor, when used singularly, has a certain level of assurance. Combining multiple authentication factors helps achieve a higher level of assurance. However, multiple authentication factors will also result in inconveniencing residents and would increase the cost of authentication. UIDAI recognizes that different service agencies may require different authentication factors / combination of authentication factors based in the characteristics of its beneficiaries, authentication environment and other service delivery needs, risks and challenges.

Based on authentication factor chosen (single or multiple) and the authentication environment available, UIDAI proposes to have multiple authentication offerings.

In addition to the above, UIDAI will also suggest authentication mechanisms for people with biometric exceptions (such as people with no fingers, totally worn out fingerprints, leprosy patients etc.)

The onus of choosing an authentication offering would lie with the AUA. UIDAI may provide tools/guidelines to assist AUAs in identifying appropriate authentication offering. However, an AUA should exercise its judgment & choose the authentication offering deemed most suitable to its service delivery / business objectives. While evaluating the risks of incorrect authentication vs. resident inconvenience, the AUAs will be advised to consider authentication offering & associated risks of current authentication mechanism or lack of it. The AUA should also consider alternate/backup authentication mechanism for possible limitations of the selected authentication offering.

7 Legal & Contractual Framework

The authentication service being offered by UIDAI will be governed by the proposed National Identification Authority of India as and when setup after enactment of the legislation.

CIDR will return only “Yes” or “No” for all authentication requests received. Ensuring privacy of the residents, UIDAI will not divulge demographic or biometric details of the residents to the AUA; it will only confirm the match / non match of data sent to CIDR.

It is also proposed to maintain transaction logs of authentication requests which the CIDR will store as required by various Laws of Land.

AUAs would be required to ensure that Aadhaar authentication is used only for lawful purposes. UIDAI will not be responsible for the purpose for which an AUA may use the authentication.

Necessary rules & regulations will also be framed keeping in view the various privacy and security needs and other Laws of Land.

To operationalize authentication, UIDAI would need to engage with various members of the ecosystem. UIDAI will enter into contract with service providers that directly manage OR connect to the CIDR.

1. UIDAI & MSP/AuSP
2. UIDAI and the AUA
3. UIDAI and the ASA

The objective of these agreements would be to detail out the roles & responsibilities, limitation, liabilities, penalties etc. of the agreeing parties.

The AUA in turn is expected to have contractual agreements with merchants / terminals, authentication usage agreement with residents. AUA may also have contractual agreements with other members of ecosystem such as device suppliers & network service provider.

UIDAI will be developing model contracts for agreement between various parties.

8 Charging Policy

Until December 2013, as a public good, Aadhaar authentication will initially be offered free of cost. Thereafter, after due consultations with various stakeholders, UIDAI will put together a charging policy keeping in view the cost incurred by UIDAI and the monetary benefit by the AUAs.

9 Risks

UIDAI is conscious of the following risks:

- Unprecedented offering – UIDAI project is unprecedented not only in terms of scale but also with respect to technology, geographic spread and socio-economic diversity. There is no parallel framework that UIDAI can easily adopt for developing its solution. In addition, biometric authentication on such a large scale for delivering social welfare programs will be deployed for the first time ever.
- Developing ecosystem – Some key requirements for adoption of Aadhaar authentication is ubiquitous network availability and robust devices capable of working under extreme weather conditions at reasonable prices. UIDAI would need to work very closely with various ecosystem members to ensure penetration of Aadhaar authentication to the target group – the unreached and the marginalized.
- Biometric authentication is dependent on a number of variables at physical environment level, device end and server end. While UIDAI may be able to control, measure and predict some of the variables at server end, same may not be possible at physical environment & device end.
- Limitations of biometrics – Like all technologies, biometric authentication too has technical limitations such as false accepts & false rejects, spoofing of identity, man-in-middle attacks etc. UIDAI would need to develop mechanism to manage some of the limitations of biometric technology.

UIDAI would constantly keep abreast of the technological advancements to handle these risks and look for ways to mitigate these risks for which UIDAI has set up the UBCC.

10 Enabling Adoption of Aadhaar Authentication

The pro-poor impact of Aadhaar will gain traction when Aadhaar authentication is linked with actual service delivery. A clear adoption process of Aadhaar authentication at every point of service delivery is critical for achieving the UIDAI mandate.

To ensure this, the UIDAI will not only work with Registrars who do enrolment, but also with non-enrolling, service delivery agencies. UIDAI is offering following assistance to various service delivery agencies to enable early adoption of Aadhaar Authentication:

- ICT assistance – UIDAI is offering financial assistance to various State governments & Central Ministries who may need to build up additional ICT infrastructure for Aadhaar enabling their service delivery.
- Technical assistance – Most of the programs in the country are driven by State Governments and there is a large variation in the current implementation status and field level requirements. UIDAI will be extending technical assistance in the form of:
    - Empanelment of consultant & software development firms that understand Aadhaar authentication & who can help various service delivery agencies to reengineer their processes and/or technology for Aadhaar enablement
    - Development of sample applications that can be used by interested by service delivery agencies

- Development of common platform elements / building blocks such as Aadhaar Payments Bridge for enabling financial transactions using authentication services.

- To promote adoption of Aadhaar authentication, the service is made free of cost for all service agencies for first 3 years. In addition, since the project is a Government of India initiative, the authentication service will be free of cost for all times for various government programs.

11 Conclusion

Aadhaar Authentication Services will bring about a transformation in the method of service delivery. It will create a circle of trust between the service provider and the resident. The service provider will have a basis to trust residents who claim to be who they are and the residents will be assured that no one can deny them their entitlements or wrongfully take their share.

The Aadhaar authentication service aims to judiciously balance the need to protect residents while empowering them. The authentication service will serve as an equalizer between residents currently excluded due to low literacy levels, high gender biases etc. on the one hand and the technology savvy residents on the other.

Anytime, anywhere, anyhow authentication ability of the Aadhaar number and Aadhaar Authentication Services will help create this circle of trust that in turn will eliminate duplication, leakages of resources and efforts, facilitate mobility and portability of identity and give the poor and rural residents the same flexibility and ease that urban non-poor residents presently have in verifying their identity and accessing services.

Circle of Trust

12 Glossary

Aadhaar Authentication	Process wherein Aadhaar number, along with other attributes is submitted to CIDR for its verification and such repository verifies the correctness thereof on the basis of information or data available with it
ASA	Authentication Service Agencies are entities that transmit authentication requests to the MSP/AuSP on behalf of one or more AUAs.
AUA	Authentication User Agencies are authorized entities such as banks, telecom companies, government departments etc. who would use CIDR authentication services
AuSP	Authentication Service Providers are entities proposed to be created that will provide CIDR based authentication services to various authentication user agencies.
CIDR	Central Identities Data Repository is the central technology infrastructure required to issue Aadhaar numbers, update resident information, and authenticate the identity of residents
CIDR	Central Identities Data Repository is the central technology infrastructure required to issue Aadhaar numbers, update resident information, and authenticate the identity of residents
DDSVP	Demographic Data Standards and Verification procedure (DDSVP) Committee Report that prescribes standards and verification procedures for carrying out UIDAI enrolments
Enrolment	Process for capturing a resident's data and issuing an Aadhaar number
FAR	False Accept Rate – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.
FRR	False Reject Rate – the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
PoA	Proof of Address document to be provided at the time of enrolment / updation
PoI	Proof of Identity document to be provided at the time of enrolment / updation
Registrar	Any entity authorized by UIDAI for the purpose of enrolling residents
Updation	Process for residents to update their demographic/biometric data present in CIDR

UIDAI Biometric Device Specifications (Authentication)

BDCS(A)-03-08

STQC - IT Services

STQC Directorate, Department of Information Technology,
Ministry of Communications & Information Technology,
Electronics Niketan, 6 CGO Complex, Lodi Road,
New Delhi – 110003

Issue 2 May 2012

SINGLE FINGER PRINT SCANNER FOR AUTHENTICATION

Parameters	**Specification**
Minimum Platen Area	**Optical/multispectral/capacitance technology** **1. If platen area is 15.24 mm x 20.32 mm or more:** **1.**1 Provisional certificate would be issued without any fied testing; 1.2 Final certification would be subject to sensor-extractor meeting <2% FRR in Aadhaar athentication system (at FAR of 0.01%) for which detailed guidelines will be published by STQC. 2. If platen area is 12.8 mm x 16.5 mm or more but less than 15.24 mm x 20.32 mm, certification would be suject to sensor-extractor meeting <2% FRR in Aadhaar authentication system (at FAR of 0.01%) for which detailed guidelines will be published by STQC. **Any other Technologies** **3. <**2% FRR in Aadhaar authentication set up (at FAR of 0.01%) would need to be demonstrated. Detailed guidelines and other requirements specific to the technology will published separately by STQC.
Image quality	Must be listed on "IAFIS Certified Product List" posted on https//www.fbibiospecs.org/IAFIS/Default.aspx under "PIV Single Finger Capture Devices" **OR** Lab Test conformance report showing compliance to ISO 19794-4 Annexure A **OR** any other equivalent conformance report (to be approved for equivalence by expert committee appointed by Competent Authority
Extractor Quality	• MINEX compliance • Number of Minutiae generated by extractor to be in conformance to ISO Specification. Tested for at least 12 Minutiae points generated under test conditions.
NFIQ Quality Software	Inbuilt NFIQ quality software either at device level or extractor level.

Parameters	**Specification**
Resolution	Minimum 500 DPI with 5% margin on the lower side
Grey scale/ Image type	8 bit, 256 levels
Extractor & Image Template Standard	ISO 19794-2 for fingerprint minutiae template and ISO 19794-4 for Fingerprint Image Template
Latent detection	Preferable
Platen	Rugged, minimum IP 54 rating preferable Prefer scratch resistant features
Preferred Operating Temperature	0 to 45 degree Centigrade
Preferred Storage Temperature	0 to 50 degree Centigrade
Preferred Humidity	10 to 90%
ESD	>= 8Kv
Environment, health and safety	ROHS certification
Safety	UL or IEC60950 compliance
EMC compliance	FCC class A or equivalent
Operating system environment	Vendor needs to declare the compatible operating system
Connectivity	1. Standard USB connectivity for PC based application. 2. Connectivity for POS devices.

Note: These specifications are subject to change based on field findings.

The biometric authentication devices from the suppliers mentioned below have been certified:

1.

Supplier	Access Computech Pvt. Ltd., 504/6, GIDC Industrial Estate, Makarpura, Vadodara – Gujarat – 390 010
Contact Details	Contact Person : Mr. Ajay Sinha Mobile No. 09327238565 Phone: +91-265-2633307, 2642978 Fax: 265-263 3268 email: ajay@acpl.ind.in
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 FM 220 CMOS STARTEK ISO/IEC 19794-2 Template Extractor Ver No:1.0.0 USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	Startek Engineering Incorporated 3F, 54, Park Ave.II, Science Based Industrial Park Hsinchu, Taiwan. R.O.C
Certificate No.	UIDAI-BDCS-AUTH-ACL-FPS-18
Valid upto	04-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

2.

Supplier	Anaxee Technologies Pvt. Ltd 74,Dhar Kothi Compound #9,Ekta Apartment, Opp. St. Raphael's Girls H.S School, Indore(M.P)-452 001
Contact Details	Contact Person: Mr. Govind Agarwal, Fax No.: 0731-2701333, Mobile: 09630020005, email: govind@anaxeetech.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Futronic FS88 Futronic FS88 Neurotechnology USB IF compliance IP54,Liveness Detection and Latent Detection - Test not

	done on the request of applicant as these are optional test
Manufacturer	Futronic Technology Co. Ltd Room 1016A, Profit Industrial building. 1-15 Kwai Fung St, Kwai Fong,N.T.,Hong Kong Tel-852-24087705 Fax-852-24197874
Certificate No.	UIDAI-BDCS-AUTH-ANX-FPS-14
Valid upto	31-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

3.

Supplier	Anaxee Technologies Pvt. Ltd 74,Dhar Kothi Compound #9,Ekta Apartment, Opp. St. Raphael's Girls H.S School, Indore(M.P)-452
Contact Details	Mr. Govind Agarwal Fax No.: 0731-2701333, Mobile: 09630020005, email: govind@anaxeetech.com
Device	Finger print scanner
Scope ***Model*** ***Sensor*** ***Extractor***	 FS88 Futronic FS88 Warwick Warp SDK 3.0 USB IF compliance Liveness Detection, Latent Detection ,IP54 - Tests not done on the request of client
Manufacturer	Futronic Technology Co. Ltd Room 1016A, Profit Industrial building. 1-15 Kwai Fung St, Kwai Fong,N.T.,Hong Kong Tel-852-24087705 Fax-852-24197874
Certificate No.	UIDAI-BDCS-AUTH-ANX-FPS-29
Valid upto	31-12-2016
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

4.

Supplier	M/s BioEnable Technologies Pvt. Ltd. Office No: 203, 2nd Level, Tower S4, Cyber City, Magarpatta city, Hadapsar, Pune-411013 Ph: (020)-65600600 Email:sales@bioenabletech.com
Contact Details	Mr. Mahesh Ghatge, (CTO) Phone : 020-66813771 Email: mg@bioenabletech.com
Device	Single Finger Capture (Authentication) Device

Scope *Model* *Sensor* *Extractor*	 Nitgen/eNBioScan-C1 HFDU08 FDU08 OPU08 Nitgen-eNBSP SDK Ver 4.8 IP54 Compliance Liveness Detection, Latent Detection - Test not done on the request of applicants as these are optional test
Manufacturer	Nitgen & Company Co. Ltd., B-12F Pax Tower, 231-13 Nonhyeon-dong Gangnam-gu Seoul REPUBLIC OF KOREA
Certificate No.	UIDAI-BDCS-AUTH-BTL-FPS-16
Valid upto	30-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

5.

Supplier	Geodesic Limited B-3, Lunic Industries, Cross Road 'B', MIDC, Andheri East, Mumbai – 400 093
Contact Details	Mr. Arnav Ganguly Head, Sales & Business Development Phone – 91-22-40786099 Fax – 91-22-28200832 Mobile:09811633984 Email: arnab.ganguly@geodesic.com rackesh.langer@geodesic.com Webpage-www.geodesic.com ; www.geoamida.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Biomini Plus SFU500/OH Suprema SFcore ver. 1.0 USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	Suprema Inc., 16F, Park view Office tower, Jeongia-Dong, Bundang-gu, Seongnam, Gyeonggi, 463-863 Korea, Tel: +82-31-783-4502
Certificate No.	UIDAI-BDCS-AUTH-GE-FPS-32
Valid upto	31-01-2016
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

6.

Supplier	Inspira Biometrics Pvt. Ltd., 23, Level 2, Kalpataru Square, Kondavita Lane, Ramakrishna Mandir Road, Andheri East, Mumbai - 400 059
Contact Details	Contact Person: Mr. Ajay Sarin, COO Phone No: 011-40576283 Fax: 011-40576286 Mobile: 09999415022 email: sales@inspira.co.in
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 CSD200 3M Cogent CSD200 Ver No:7.10 USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	3M Cogent, Inc. 639 N, Rosemead Bvld. Pasadena, C A 91107, USA
Certificate No.	UIDAI-BDCS-AUTH-IBL-FPS-02
Valid upto	04-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

7.

Supplier	Integra Micro Systems (P) Ltd., G-5, Swiss Complex, 33 Race Course Road Bangalore – 560 001
Contact Details	Mr. Bidyut K. Das Regional Manager – North & East Phone +91-11-47671304, 080- 2250073/2257027 080-32715046, (M) 9818638063 Fax - +91-11-47671315 Email: bkdas@integramicro.com
Device	USB based Single fingerprint Scanner
Scope **Model** **Sensor** **Extractor**	 Futronic FS88 Futronic FS88 Innovatrics Ver. 1.56 USB IF compliance Liveness Detection, Latent Detection,IP54- Test not done on the request of applicant as these are optional test
Manufacturer	Futronic Technology Co. Ltd Room 1016A, Profit Industrial building. 1-15 Kwai Fung St,

	Kwai Fong,N.T.,Hong Kong Tel-852-24087705 Fax-852-24197874
Certificate No.	UIDAI-BDCS-AUTH-IMS-FPS-11
Valid upto	30-01-2016
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

8.

Supplier	Mantra Softech India Pvt. Ltd C3,Blue Heaven Complex, SP Colony Road Naranpura ,Ahmedabad,380013 Gujarat India
Contact Details	Hiren Bhandari Mobile No.: +91 9327020417 Tel.NO.: + +91-79-64506243 - 79-66051243 (Fax) Email: hiren@mantratec.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Mantra/MFS100 Sensor – MOPv1.1 Iengine_ansi_iso, Innovatrics version 1.55 USB IF compliance IP54 compliance Liveness Detection, Latent Detection - Test not done on the request of appliacant as these are optional test
Manufacturer	Mantra Softech India Pvt. Ltd C3,Blue Heaven Complex, SP Colony Road Naranpura ,Ahmedabad,380013 Gujarat India
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-04-FC
Valid upto	30-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

9.

Supplier	NEC India PVT.Ltd 2nd floor, Plot no. 7, TDI centre, Jasola District Centre New Delhi – 110 025 Tel-011 61101000 Fax-011 61101001
Contact Details	Mr. Pradeep Kushwaha, Head - Public Safety Phone + 91-11-61101000

	(M) + 91 8800795323 Fax: +91 - 11-61101001 Email: www.necindia.in, pradeepkushwaha@necindia.in
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Futronic FS88 Futronic FS88 Neurotechnology USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	Futronic Technology Co. Ltd Room 1016A, Profit Industrial building. 1-15 Kwai Fung St, Kwai Fong,N.T.,Hong Kong Tel-852-24087705 Fax-852-24197874
Certificate No.	UIDAI-BDCS-AUTH-NEC-FPS-56
Valid upto	31-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

10.

Supplier	NEC India PVT.Ltd 2nd floor, Plot no. 7, TDI centre, Jasola District Centre New Delhi – 110 025 Tel-011 61101000 Fax-011 61101001
Contact Details	Mr. Pradeep Kushwaha, Head - Public Safety Phone + 91-11-61101000 (M) + 91 8800795323 Fax: +91 - 11-61101001 Email: www.necindia.in, pradeepkushwaha@necindia.in
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Mantra/MFS100 Sensor – MOPv1.1 Iengine_ansi_iso, Innovatrics version 1.55 USB IF compliance IP54 compliance Liveness Detection, Latent Detection - Test not done on the request of appliacant as these are optional test
Manufacturer	Mantra Softech India Pvt. Ltd C3,Blue Heaven Complex, SP Colony Road

	Naranpura ,Ahmedabad,380013 Gujarat India
Certificate No.	UIDAI-BDCS-AUTH-NEC-FPS-59
Valid upto	30-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

11.

Supplier	Precision Infomatic (M) Pvt. Ltd., #22, Habibullah Road, T.Nagar, Chennai - 600 017. Tamil Nadu.
Contact Details	Contact Person: Mr. Mathew Chacko (Director) Phone No. ; 044-42199500 Fax No.: 044-42199502, Mobile No.: 09940635323 email: mathew@precisionit.co.in
Device	Optical based Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 CSD200 3M Cogent CSD200 InnalT v 1.3.0.1 USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	3M Cogent, Inc. 639 N, Rosemead Bvld. Pasadena, C A 91107, USA
Certificate No.	UIDAI-BDCS-AUTH-PIL-FPS-04
Valid upto	04-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

12.

Supplier	Sagem Morpho Security Pvt. Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director

	Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO1350E CBME Morphosoft Embedded (Ver.V9) USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-01-FC
Valid upto	06-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

13.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO1300E CBME Morphosoft Embedded (Ver.V9) IP54 Compliance USB IF compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-02-FC

Valid upto	06-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

14.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO1350E2 CBME2 Morphosoft Embedded (Ver.V9) USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test.
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-03-FC
Valid upto	09-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

15.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 300 MSO OEM Morphosmart Embedded (Ver.V9)

	IP54 Compliance USB IF compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-08-FC
Valid upto	26-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

16.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 301 MSO OEM XX1 Morphosmart Embedded (Ver.V9) IP54 Compliance USB IF compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-09-FC
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

17.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director

	Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 1350 E MSO CBME Morphokit (Ver.V6) USB IF Compliance Liveness Detection, Latent Detection, IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-10-FC
Valid upto	21-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

18.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 1300 E MSO CBME Morphokit (Ver.V6) IP54 Compliance USB IF compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-11-FC
Valid upto	21-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

19.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 1350 E2 MSO CBM E2 Morphokit (Ver.V6) USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-12-FC
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

20.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 300 MSO OEM Morphokit (Ver.V6) IP54 Compliance USB IF compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc

	75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-13-FC
Valid upto	26-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

21.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO 301 MSO OEM XX1 Morphokit (Ver.V6) IP54 Compliance USB IF compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-14-FC
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

22.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO1300E2 CBME2 MorphoSoft Embedded (Ver.V9)

	USB IF compliance IP54 compliance Liveness Detection, Latent Detection - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-44
Valid upto	02-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

23.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO1300E2 CBME2 Morphokit (Ver.V6) USB IF compliance IP54 compliance Liveness Detection, Latent Detection, IP54 - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-49
Valid upto	02-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

24.

Supplier	Sagem Morpho Security Pvt.Ltd.

	Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO350 MSO OEM MorphoSoft Embedded (Ver.V9) USB IF compliance Liveness Detection, Latent Detection, IP54 - Test not done on the request of applicant as these are optional test.
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-8.3
Valid upto	02-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

25.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO350 MSO OEM Morphokit (Ver.V6) USB IF compliance Liveness Detection, Latent Detection, IP54 - Test not done on the request of applicant as these are optional test.
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France

Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-50
Valid upto	16-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

26.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 Morpho/MSO351 MSO OEM XX1 MorphoSoft Embedded (Ver.V9) USB IF compliance Liveness Detection, Latent Detection, IP54 - Test not done on the request of applicant as these are optional test.
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-8.4
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

27.

Supplier	Sagem Morpho Security Pvt.Ltd. Suit No. 18-20, 9th Floor Hindustan Times Building Kasturba Gandhi Marg,New Delhi-110001
Contact Details	Ujjwal Sabharwal Product Management Director Mobile No.: +91 78 38 66 60 52 Tel.NO.: +91 11-4355-1514/55(Fax) Email: ujjwal.sabharwal@morpho.com
Device	Single Finger Capture (Authentication) Device

Scope *Model* *Sensor* *Extractor*	 Morpho/MSO351 MSO OEM XX1 Morphokit (Ver.V6) USB IF compliance Liveness Detection, Latent Detection, IP54 - Test not done on the request of applicant as these are optional test.
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-51
Valid upto	02-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

28.

Supplier	Secugen India Pvt. Ltd. Unit No. 605-608, C Wing Solaris 1, Saki Vihar Road,Andheri East,Mumbai, Maharashtra
Contact Details	Contact Person :Mr. Himanshu Shah Mobile No. 09820100778 Phone: +91 22 2847 8472 Fax-+91 22 2847 8479 email: himanshu@secugenindia.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 HU20 U20 SECUGEN-SGFPM, Ver No: 3.5.4.2 IP54 compliance Liveness Detection, Latent Detection, Durability - Test not done on the request of applicant as these are optional test
Manufacturer	Secugen Corporation, 2065,Martin Avenue, Suite 108, Santa Clara, Calie 95050, USA
Certificate No.	UIDAI-BDCS-AUTH- SEC-FPS- 61
Valid upto	03-04-2017
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

29.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301

Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 1300 E CBM-E EmbeddedV9 USB IF compliance IP54 compliance Liveness Detection and Latent Detection, - Test not done on the request of applicant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France
Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-03
Valid upto	06-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

30.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 1350 E CBM-E MorphoSoft Embedded, Morpho make V9 USB IF compliance Liveness Detection, Latent Detection,IP54 - Test not done on the request of appliacant as these are optional test
Manufacturer	MORPHO – Le Ponant de Paris 27 Rue Leblanc 75012 Paris Cedex 15, France

Certificate No.	UIDAI-BDCS-AUTH-SMS-FPS-03
Valid upto	06-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

31.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 300 Morpho/MSO OEM MorphoSoft Embedded V9 USB IF compliance IP54 Compliance Liveness Detection, Latent Detection - Test not done on the request of appliacant as these are optional test
Manufacturer	Morpho- 11 Boulevard Gallieni FR92130 ISSY LES MOULINEAUX
Certificate No.	UIDAI-BDCS-AUTH-SCL-FPS-7.1
Valid upto	26-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

32.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com

Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 301 MSO OEM XXI MorphoSoft Embedded V9 USB IF compliance IP54 compliance Liveness Detection, Latent Detection- Test not done on the request of appliacant as these are optional test
Manufacturer	Morpho- 11 Boulevard Gallieni FR92130 ISSY LES MOULINEAUX
Certificate No.	UIDAI-BDCS-AUTH-SMS-SCL-7.2
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

33.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 350 MSO OEM MorphoSoft Embedded, V9 USB IF compliance Liveness Detection, Latent Detection,IP54 - Test not done on the request of appliacant as these are optional test
Manufacturer	Morpho- 11 Boulevard Gallieni FR92130 ISSY LES MOULINEAUX
Certificate No.	UIDAI-BDCS-AUTH-SCL-FPS-7.3
Valid upto	02-12-2015

Reference	BDCS(A)-03-01 and BDCS(A)-03-08

34.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 351 MSO OEM XXI MorphoSoft Embedded V9 USB IF compliance Liveness Detection, Latent Detection,IP54 - Test not done on the request of appliacant as these are optional test
Manufacturer	Morpho- 11 Boulevard Gallieni FR92130 ISSY LES MOULINEAUX
Certificate No.	UIDAI-BDCS-AUTH-SCL-FPS-7.4
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

35.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device

Scope *Model* *Sensor* *Extractor*	 MSO 1300 E2 CBME2 MorphoSoft Embedded, Morpho make V9 USB IF compliance IP54 compliance Liveness Detection, Latent Detection - Test not done on the request of appliacant as these are optional test
Manufacturer	Morpho- 11 Boulevard Gallieni FR92130 ISSY LES MOULINEAUX
Certificate No.	UIDAI-BDCS-AUTH-SCL-FPS-52
Valid upto	11-10-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

36.

Supplier	Smart Chip Ltd., D-216, Sector -63, Noida-201301
Contact Details	Mr. Pankaj Aggarwal,, Phone: 0120-4699900 Fax No.: 0120-4699901 Mobile 09899600929 e-mail: pankaj.agarwal@smartchiponline.com
Device	Single Finger Capture (Authentication) Device
Scope *Model* *Sensor* *Extractor*	 MSO 1350 E2 CBME2 MorphoSoft Embedded V9 USB IF compliance Liveness Detection, Latent Detection,IP54 - Test not done on the request of appliacant as these are optional test
Manufacturer	Morpho- 11 Boulevard Gallieni FR92130 ISSY LES MOULINEAUX
Certificate No.	UIDAI-BDCS-AUTH-SCL-FPS-54
Valid upto	09-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

37.

Supplier	Smart Identity Devices Pvt. Ltd., B-37, Polyplex Complex, Sector -1 Noida-201301
Contact Details	Mr. Nirmal Prakash/Mr. Ankur Saluja, Phone: 0120-2442192 Fax No.: 0120-2442191 Mobile 09312068975/9310066033 e-mail: md@smartid.in, sales@smartid.in
Device	USB based Single fingerprint Scanner
Scope *Model* *Sensor* *Extractor*	 Futronic FS-88 Futronic FS-88 Neurotechnology USB IF compliance Liveness Detection, Latent Detection,IP54 Durability - Test not done on the request of applicant as these are optional test
Manufacturer	Futronic Technology Co. Ltd Room 1016A, Profit Industrial building. 1-15 Kwai Fung St, Kwai Fong,N.T.,Hong Kong Tel-852-24087705 Fax-852-24197874
Certificate No.	UIDAI-BDCS-AUTH-SID-FPS-09
Valid upto	31-12-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

38.

Supplier	Smart Identity Devices Pvt. Ltd., B-37, Polyplex Complex, Sector -1 Noida-201301
Contact Details	Mr. Nirmal Prakash/Mr. Ankur Saluja, Phone: 0120-2442192 Fax No.: 0120-2442191 Mobile 09312068975/9310066033 e-mail: md@smartid.in, sales@smartid.in
Device	USB based Single fingerprint Scanner
Scope *Model* *Sensor* *Extractor*	 Eikon Touch 500 TCS1S Innovatrics V1.55 USB IF compliance Liveness Detection, Latent Detection,IP54- Test not done on the request of applicant as these are optional test

Manufacturer	Authentec, Inc. 100, Rialto Place, Suite 100, Melbourne, Florida 32901 (USA)
Certificate No.	UIDAI-BDCS-AUTH-SID-FPS-19
Valid upto	30-01-2016
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

39.

Supplier	Smart Identity Devices Pvt. Ltd., B-37, Polyplex Complex, Sector -1 Noida-201301
Contact Details	Mr. Nirmal Prakash/Mr. Ankur Saluja, Phone: 0120-2442192 Fax No.: 0120-2442191 Mobile 09312068975/9310066033 e-mail: md@smartid.in, sales@smartid.in
Device	USB based Single fingerprint Scanner
Scope *Model* *Sensor* *Extractor*	 Biomini Plus SFU500/OH Neurotechnology Ver 4.3 USB IF compliance Liveness Detection, Latent Detection,IP54- Test not done on the request of appliacant as these are optional test
Manufacturer	Suprema Inc., 16 F, Park View Office Tower, Jeongia-Dong, Bundang-Gu Seongnam, Korea
Certificate No.	UIDAI-BDCS-AUTH-SID-FPS-20
Valid upto	30-01-2016
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

40.

Supplier	Smart Identity Devices Pvt. Ltd., B-37, Polyplex Complex, Sector -1 Noida-201301
Contact Details	Mr. Nirmal Prakash/Mr. Ankur Saluja, Phone: 0120-2442192 Fax No.: 0120-2442191 Mobile 09312068975/9310066033 e-mail: md@smartid.in, sales@smartid.in sales@smartid.in
Device	USB based Single fingerprint Scanner
Scope **Model** **Sensor** **Extractor**	 U.are.U 4500 Fingerprint reader U.are.U 4500 UID Edition Sensor Digital Persona, Fingerjet Ver 5.2 USB IF compliance Liveness Detection, Latent Detection,IP54- Test not done

	on the request of applicant as these are optional test
Manufacturer	Digital Persona Inc., 720 Bay Road, Redwood city, CA 94063, USA
Certificate No.	UIDAI-BDCS-AUTH-SID-FPS-26
Valid upto	30-01-2016
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

41.

Supplier	Smart Identity Devices Pvt. Ltd., B-37, Polyplex Complex, Sector -1 Noida-201301
Contact Details	Mr. Nirmal Prakash/Mr. Ankur Saluja, Phone: 0120-2442192 Fax No.: 0120-2442191 Mobile 09312068975/9310066033 e-mail: md@smartid.in, sales@smartid.in
Device	USB based Single fingerprint Scanner
Scope *Model* *Sensor* *Extractor*	 Real Scan–G1 Real Scan-G1 Ver V01B Neurotech Ver 4.2 USB IF compliance Liveness Detection, Latent Detection,IP54- Test not done on the request of appliacant as these are optional test
Manufacturer	Suprema Inc., 16 F, Park View Office Tower, Jeongia-Dong, Bundang-Gu Seongnam, Korea
Certificate No.	UIDAI-BDCS-AUTH-SID-FPS-21
Valid upto	30-09-2015
Reference	BDCS(A)-03-01 and BDCS(A)-03-08

The Certificate of Approval is based on STQC Biometric Device Certification Scheme (document no.BDCS(A)-03-01 Issue 1 on "Rules and Procedures for Testing and Certification of Biometric Devices for UID Application)
This approval is subject to satisfactory compliance of surveillance visits, test reports and validity of support certifications.

List last updated on -Ver2.1.1 dated 10.02.2015

******

The biometric authentication devices-IRIS from the suppliers mentioned below have been certified:

1.

Supplier	Biometronic Technology Pvt. Ltd. Pyramid North Square 109/1B,First floor, third division , Nehru Nagar, On International airport road, Yelahanka, Banglore-560064 Ph-080-6565 7615, 2846 0229 Email: info@biometronic.com Corporate office-Flat no.-30,Shri Hari apartment,Sector-12,Plot No.6,Dwarka,New Delhi-110075
Contact Details	Mr. Prabhu Sridharan Tel.NO.: +91 9945551410 Email: prabhu@biometronic.com
Device	IRIS (Authentication) Device
Scope *Model* *Sensor* *REFERENCE NO.-* Module No.	 IRISHIELD TM –USB MK2120U OV7725 IRISHIELD M2120
Platform/OS	Windows 7 & XP
Manufacturer	IRITECH, Inc. Suite 701,Cheongdong Bldg.,1922,Nambusunhwan –ro,Gwanak-gu,Seoul 151-832,Korea Manufacturing location- Sambon Precision & Electronics Co.,Ltd 204,Samjeong–dong,Ojeong-gu,Bucheon-city,Kyeonggi-do,Korea Corporate office-IRITECH Inc., 3951 pender Dr. suite 120A Fairfax,VA22030, U.S.A
Certificate No.	UIDAI/BDCS/IRIS/BIOMETRONIC/06
Valid upto	21.01.2017
Reference	BDCS(A-I)-03-02 and BDCS(A-I)-03-07

2.

Supplier	Biometronic Technology Pvt. Ltd. Pyramid North Square 109/1B,First floor, third division , Nehru Nagar, On International airport road, Yelahanka, Banglore-560064 Ph-080-6565 7615, 2846 0229 Email: info@biometronic.com Corporate office-Flat no.-30,Shri Hari apartment,Sector-12,Plot No.6,Dwarka,New Delhi-110075
Contact Details	Mr. Prabhu Sridharan Tel.NO.: +91 9945551410 Email: prabhu@biometronic.com
Device	IRIS (Authentication) Device
Scope *Model* *Sensor* *REFERENCE NO.-* Module No.	 IRISHIELD–USB BK 2121U OV7725 IRISHIELD B2121
Platform/OS	Windows 7 & XP
Manufacturer	IRITECH, Inc. Suite 701,Cheongdong Bldg.,1922,Nambusunhwan –ro,Gwanak-gu,Seoul 151-832,Korea Manufacturing location- Sambon Precision & Electronics Co.,Ltd 204,Samjeong–dong,Ojeong-gu,Bucheon-city,Kyeonggi-do,Korea Corporate office-IRITECH Inc., 3951 pender Dr. suite 120A Fairfax,VA22030, U.S.A
Certificate No.	UIDAI/BDCS/IRIS/BIOMETRONIC/05
Valid upto	21.01.2017
Reference	BDCS(A-I)-03-02 and BDCS(A-I)-03-07

Supplier	Biometronic Technology Pvt. Ltd. Pyramid North Square 109/1B,First floor, third division , Nehru Nagar, On International airport road, Yelahanka, Banglore-560064 Ph-080-6565 7615, 2846 0229 Email: info@biometronic.com Corporate office-Flat no.-30,Shri Hari apartment,Sector-12,Plot No.6,Dwarka,New Delhi-110075
Contact Details	Mr. Prabhu Sridharan Tel.NO.: +91 9945551410 Email: prabhu@biometronic.com
Device	IRIS (Authentication) Device
Scope *Model* *Sensor* *REFERENCE NO.-* Module No.	 IRIHERALD 1000MK OV7725 IRIHERALD 1000M
Platform/OS	Windows 7 & XP
Manufacturer	IRITECH, Inc. Suite 701,Cheongdong Bldg.,1922,Nambusunhwan –ro,Gwanak-gu,Seoul 151-832,Korea Manufacturing location- Sambon Precision & Electronics Co.,Ltd 204,Samjeong–dong,Ojeong-gu,Bucheon-city,Kyeonggi-do,Korea Corporate office-IRITECH Inc., 3951 pender Dr. suite 120A Fairfax,VA22030, U.S.A
Certificate No.	UIDAI/BDCS/IRIS/BIOMETRONIC/04
Valid upto	21.01.2017
Reference	BDCS(A-I)-03-02 and BDCS(A-I)-03-07

Supplier	Biomatiques Identification Solutions Pvt. Ltd. G5,Ashray Building ,Opp. Govindji Park-A,Umra,Surat-395 007,Gujarat,India
Contact Details	Mr. Pratik. N Patel(Project Manager) Tel.NO.: +91 9909804321 email: pratik@biomatiques.com
Device	IRIS (Authentication) Device
Scope *Model* *Sensor* *REFERENCE NO.-* Module No.	EPI-1000 BIS-7725OV BIS-101C
Platform/OS	Windows 7 & XP
Manufacturer	Biomatiques Identification Solutions Pvt. Ltd. G5,Ashray Building ,Opp. Govindji Park-A,Umra,Surat-395 007,Gujrat,India
Certificate No.	UIDAI/BDCS/IRIS/BIOMATIQUE/01
Valid upto	25.12.2017
Reference	BDCS(A-I)-03-02 and BDCS(A-I)-03-07

The Certificate of Approval is based on STQC Biometric Device Certification Scheme (document no.BDCS(A-I)-03-02 Issue 1 on Procedure for obtaining Biometric device Certification (IRIS Authentication) for UID Application)
This approval is subject to satisfactory compliance of surveillance , test reports and validity of support certifications.

Unique Identification
Authority of India

Aadhaar Holder Consent Form Illustrative Template

The below illustrative template for obtaining consent from the Aadhaar holder for using the Aadhaar number, Biometric information and/or One Time Pin (OTP) for providing the Aadhaar Authentication Service to be used by an Authentication User Agency(AUA). AUA may customize the consent form as per their requirement.

___<Name of Agency providing the service>___

Consent for Authentication

[ ] *Mark a tick (√) to provide consent to below option*

I hereby state that I have no objection in authenticating myself with Aadhaar based authentication system and consent to providing my Aadhaar number, Biometric and/or One Time Pin (OTP) data for Aadhaar based authentication for the purposes of availing of the ___<mention the name of the service>___ from ___<name of agency providing the service>___.

I understand that the Biometrics and/or OTP I provide for authentication shall be used only for authenticating my identity through the Aadhaar Authentication system for that specific transaction and for no other purposes.

I understand that ___<name of agency providing the service>___ shall ensure security and confidentiality of my personal identity data provided for the purpose of Aadhaar based authentication.

OR,

[ ] *Mark a tick (√) to provide consent to below option*

I do not wish to authenticate myself with the Aadhaar based Authentication system for Authentication of my identity. However, I do understand that if at anytime I wish to authenticate myself with the Aadhaar based Authentication system I need to provide a consent to ___<name of agency providing the service>___ to provide my Aadhaar number, Biometric and/or OTP data.

Signature/Thumb Impression: _____
Name: _____
Aadhaar Number: _____
Service Agency relationship number: _____
(e.g., Bank A/C Number or Customer Id etc)
Date: ____/____/20____

CONTACT DETAILS				
Sl No	Designation	Contact Person	Phone No	email Id
1	Authentication UIDAI on Boarding & Technical Support team	AUTH SUPPORT	01123462644	Authsupport@uidai.gov.in
2	UIDAI RO Bangalore	PRASHANTH	9880899922	Prashant.hs@uidai.net.in
3	UIDAI Auth Support	MANOJ	9811887905	
4	Project Director KRDH & UID	PRABHAKAR HL	080-22230060	pd.uid@karnataka.gov.in pd.krdh@karnataka.gov.in
5	Project Manager KRDH	USHARANI K	080-22230060	pm-krdh@karnataka.gov.in
6	Process Consultant	ABHISHEK PURI	080-22230060	proc.krdh@karnataka.gov.in
7	Technical Consultant KRDH	APOORVA PRAKASH	9482565374	tc5.krdh@karnataka.gov.in
8	Technical Consultant KRDH	SAHANA GS	8762556536	tc6.krdh@karnataka.gov.in
9	Technical Consultant KRDH	NAGARAJ NM	8762556537	tc2.krdh@karnataka.gov.in