Aadhaar Authentication Overview

The Unique Identification Authority of India (UIDAI) has been created, with the mandate of providing a unique identity (Aadhaar) number to all residents of India and also defining usages and applicability of Aadhaar for delivery of various services. Towards Aadhaar-enabling delivery of various services, UIDAI proposes to provide online authentication using demographic and biometric data.

What is Aadhaar Authentication?

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic/biometrics/OTP) is 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 a “yes/no”. No personal identity information is returned as part of the response.

The purpose of Authentication is to enable residents to prove their identity and for service providers to confirm that the residents are ‘who they say they are’ in order to supply services and give access to benefits.

What Are the Expected Benefits of Aadhaar Authentication?

A. Establishing Identity:

Adding new beneficiaries – Aadhaar authentication can be used as proof of identity and proof of address to extend basic social welfare programs such as PDS & RSBY to residents. It would also give residents access to social levellers such as banking & telecom which they have so far been denied for want of identity proof.

Confirming beneficiary – Various programs where beneficiaries need to be confirmed before delivery of the service can use Aadhaar authentication. This will help curb leakages and ensure that the targeted beneficiary is not denied entitlement.

Attendance management – Programs such as SSA and NREGA where financial outlay 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 using Aadhaar authentication have the potential of changing financial landscape of the country.

Access control – Aadhaar authentication could be used to control access/entry to restricted areas such as airports, hotels, examination halls 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.

Demand-driven, portable service delivery – Since beneficiaries can authenticate their Aadhaar anywhere, 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 through self-service kiosks, mobile phones, call centres etc.

Accountability / vigilance – Aadhaar-based authentication can also be used for authenticating officials / members responsible for service delivery, audits, vigilance etc.
C. Address and Demographic Verification:

**Address verification** – Address verification, which is a key requirement for providing services like telephone connection, banking products, could be done through Aadhaar authentication. This is expected to reduce the cost of KYC & at the same time provide a reliable verification mechanism.

**Demographic data verification** – Demographic data like age and gender can be verified through Aadhaar authentication.

**Aadhaar Authentication Offerings**

- **Type 1 Authentication** – Through this offering, service delivery agencies can use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, etc) of a resident.

- **Type 2 Authentication** – This offering allows service delivery agencies to authenticate residents through One-Time-Password (OTP) delivered to resident’s mobile number and/or email address present in CIDR.

- **Type 3 Authentication** – Through this offering, service delivery agencies can authenticate residents using one of the biometric modalities, either iris or fingerprint.

- **Type 4 Authentication** – This is a 2-factor authentication offering with OTP as one factor and biometrics (either iris or fingerprint) as the second factor for authenticating residents.

- **Type 5 Authentication** – This offering allows service delivery agencies to use OTP, fingerprint & iris together for authenticating residents.

The Aadhaar number needs to be submitted in all forms of authentication so that this operation is reduced to a 1:1 match. Aadhaar number itself is not an authentication factor. Type 1 authentication may be combined with any other Aadhaar authentication offering.

Service delivery agencies should select the appropriate authentication type based on their business requirements. They would need to balance out the resident convenience and service delivery risk before finalizing the authentication offering.

---

**What Aadhaar Authentication Will Do & Will Not Do**

<table>
<thead>
<tr>
<th>What Aadhaar Authentication Will Do</th>
<th>What Aadhaar Authentication Will Not Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate against resident’s data in UIDAI’s CIDR</td>
<td>Authenticate against data stored on a smart card</td>
</tr>
<tr>
<td>Return response to requesting agencies as Yes/No</td>
<td>Return personal identity information of residents</td>
</tr>
<tr>
<td>Initiate request over mobile network, landline network and broadband network</td>
<td>Remain restricted to broadband network</td>
</tr>
<tr>
<td>Require Aadhaar for every authentication request reducing transaction to 1:1 match</td>
<td>Search for Aadhaar based on details provided requiring 1:N match</td>
</tr>
</tbody>
</table>

For further details, please visit [http://uidai.gov.in/auth](http://uidai.gov.in/auth)

For any clarifications, please contact Mr. Yashwant Kumar, ADG, UIDAI at auth.ecosys@uidai.gov.in

Aadhaar Authentication Services
Aadhaar Authentication Operating Model Overview

Key Actors in Aadhaar Authentication

**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.

**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.

**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.

**Sub AUA:** An entity desiring to use Aadhaar authentication to enable its services through an existing AUA. Examples: (i) 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.

**Authentication Devices:** 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 by the AUA/Sub AUA.

**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 actors 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.
Federated Model

UIDAI offers Aadhaar authentication that can be used alone or in conjunction with AUAs domain/application specific authentication scheme (called "federated authentication"). For example, in federated authentication, a Bank could choose to use an ATM card and fingerprint for authentication of which the ATM card is authenticated within Bank's application whereas the fingerprint is authenticated against data in the CIDR using Aadhaar authentication.

Most current authentication systems can be described as "local" (i.e., pertaining to and/or valid for a few services, situations or entities) and "revocable" (wherein an existing identity factor could be revoked and reissued as a result of expiry, compromise or other valid reasons). Aadhaar authentication system, on the other hand, could be described as "global" (because of its applicability across AUAs and services) and "non-revocable" (because Aadhaar identity factors such as fingerprints and iris scans cannot usually be revoked/replaced).

In the federated authentication model, the global-irrevocable Aadhaar authentication co-exists with and strengthens the local-revocable authentication of AUAs. Such a federated approach would result in authentication systems that are stronger and more reliable than those that are based either only on global-irrevocable model or only on local-revocable model.

While the federated model does not mandate the existence or use of an AUA's own authentication (if an AUA/Sub-AUA so wishes, they could use only Aadhaar authentication by itself), AUAs/Sub-AUA are encouraged to use Aadhaar authentication in conjunction with their existing authentication to render the overall authentication system stronger and more reliable.

Handling Network Exceptions

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.

Even though the authentication device may transmit multiple authentication requests at the same time in case multiple buffered requests are sent simultaneously, each authentication request will be treated as a separate transaction in the Aadhaar authentication system. In addition, UIDAI expects that buffering would only be done at the device level and not at AUA/ASA server end.

Handling Biometric Exceptions

As in any other technology, biometric technology too has its own limitations. There would be a very small fraction of the population with all biometrics (both fingerprint and iris) missing who may not be able to avail any biometric authentication. Further, there would be a set of people who may not be able to avail fingerprint-based authentication such as people with missing fingers, people having very poor quality fingerprints. In addition, there could be a set of people with temporary problems in biometric authentication such as cut/burnt fingers, extreme environmental conditions etc.

UIDAI recommends that AUAs opting for biometric authentication should have alternate mechanisms to service genuine residents who are not able to use biometric authentication. 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.

For further details, please visit http://uidai.gov.in/auth
For any clarifications, please contact Mr. Yashwant Kumar, ADG, UIDAI at auth.ecosys@uidai.gov.in

Aadhaar Authentication Services
Authentication User Agency (AUA)

AUA is any government / public / private legal agency registered in India that seeks to use Aadhaar authentication for its services. An AUA is the principal agency that sends authentication requests to enable its services / business functions.

An AUA connects to the CIDR through an ASA (either by becoming ASA on its own or contracting services of an existing ASA).

Examples of AUAs:

Department of Civil Supplies, which seeks to verify the identity of a target resident before issuing them their monthly ration of rice, kerosene, etc.

Any bank / financial institution that seeks to verify the identity of its customer before letting them complete a financial transaction such as withdrawal or transfer of funds.

The administration/security department of a high-security building/zone that seeks to verify the identity of any individual seeking entry into the building/zone.

AUA Readiness Stages

- Identify business / service delivery needs – The agency needs to identify service delivery areas where Aadhaar authentication may be used. The agency also needs to decide what authentication types they would be using for Aadhaar enabling different service delivery needs.

- Fill online application form – Any agency interested in becoming an AUA needs to apply online. UIDAI has an online workflow based application form for engaging with AUAs.

- Engage with ASA(s) – One of the initial stages for becoming an AUA is the need to engage with an existing ASA. The list of approved ASAs would be available online and an interested AUA can engage accordingly. In case an agency wants to become both ASA and AUA, it would first need to get approved as an ASA and then apply for becoming AUA.

- Send signed contract and supporting documents to UIDAI – The AUA should send hardcopy of the signed contract along with required supporting documents to UIDAI. The online application would be approved by UIDAI upon receipt of the required documents.

- Ensure process and technology compliance – The AUA needs to setup necessary systems, processes, infrastructure etc. in compliance with UIDAI’s standards and specifications. Some such requirements include defining exception handling mechanism, developing application using Aadhaar authentication APIs, ensuring connectivity from authentication devices to the AUA server etc. Compliance to various requirements needs to be confirmed to UIDAI through the online application form.

- Plan device deployment – The AUA needs to decide upon the authentication device specifications based on its business requirements and ensure deployment of same. If an AUA opts for biometric authentication, the sensor/extractor of the devices needs to be certified by STQC. If an AUA opts for operator-assisted devices, the AUA would also need to ensure training and readiness of operators.

- Obtain approvals from UIDAI – UIDAI would approve an AUA’s application form when various compliance requirements are met. An AUA should engage with UIDAI during the process and provide required clarifications.

- Carry out end-to-end testing – Approval from UIDAI allows an AUA to carry out end-to-end testing of their application with the CIDR. Before going live with actual resident authentication, it is highly recommended that an AUA carries out thorough end-to-end testing of their application with the selected ASA and with CIDR. The AUA should get the systems related to Aadhaar
authentication audited by information systems auditors certified by a recognized body before going live.

- **Go-live** – An AUA can go-live after confirmation of adherence to all UIDAI’s standards and specifications. UIDAI plans to manage the same through online workflow based application.

**Key AUA Responsibilities**

- Choose an appropriate authentication type based on business and deployment risk assessment; inform UIDAI regarding the same.
- Ensure compliance of authentication related operations (processes, technology, security, etc.) to UIDAI’s standards and specifications.
- Prepare authentication packet as per Authentication API specifications.
- Log and maintain details of all authentication transactions.
- In case Aadhaar biometric authentication is used, ensure Best Finger Detection (BFD) application is implemented to on-board the residents for biometric authentication.
- Identifying exception-handling and back-up identity authentication mechanisms.
- Deploy fraud monitoring mechanism, as per AUA’s business needs, to prevent misuse of exception handling mechanism by operators and any other ecosystem members.
- Get its operations and systems related to Aadhaar Authentication audited as per UIDAI’s specifications.
- Ensure connectivity from authentication devices to the AUA server and between the AUA server and the ASA server.
- Procure, deploy and manage devices in compliance with UIDAI specifications.
- Ensure adequate training for the personnel managing authentication devices.
- Inform UIDAI of the engagement/disengagement of Sub AUAs.
- Ensure supported Sub AUAs comply with UIDAI’s standards and specifications.
- Inform UIDAI of any misuse of Aadhaar data, authentication services, or any compromise of Aadhaar related data or systems.

**Mandatory Security Requirements**

- Aadhaar number should be never used as a domain specific identifier.
- In the case of operator assisted devices, operators should be authenticated using mechanisms such as password, Aadhaar authentication, etc.
- 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 short period, currently configured as 24 hours.
- Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database.
- The meta data and the responses should be logged for audit purposes.
- Network between AUA and ASA should be secure.

For further details, please visit http://uidai.gov.in/auth
For any clarifications, please contact Mr. Sameer Gupta, ADG, UIDAI at auth.ecosys@uidai.gov.in

Aadhaar Authentication Services
Authentication Service Agency (ASA)

An ASA is an agency that establishes secure leased line connectivity to the CIDR to transmit authentication request on behalf of AUAs and receive response back from CIDR. An ASA can serve more than one AUA. ASAs may also offer value added services to AUAs in addition to providing them with connectivity to CIDR. Such value added services are not managed by UIDAI.

ASA Eligibility Criteria

The agency should either be

1. A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government OR
2. An Authority constituted under the Central / State Act OR
3. A Not-for-profit company / Special Purpose organization of national importance OR
4. A company registered in India under the Indian Companies Act 1956 meeting the following requirements:
   a. Financial capabilities – An annual turnover of at least Rs. 100 crores in last three financial years, and
   b. Technical capabilities:
      i. A Telecom Service Provider (TSP) operating pan India fibre optics network and should have a minimum of 100 MPLS Points of Presence (PoP) across all states OR
      ii. Should be a Network Service Provider (NSP) capable of providing network connectivity for data, voice transmission and should have an agreement with the TSP having 100 MPLS PoPs OR
      iii. System Integrator having necessary arrangement with TSP/NSP as described above

c. The agency should not have been blacklisted by Central / State Governments / PSUs of Central / State Governments in the last five years

The agency should give an undertaking and demonstrate the capability of design, configure, implement and maintain the infrastructure and systems required for an ASA as per UIDAI’s specifications and certify that necessary human resources with requisite skills are in place to perform the functions required as an ASA.

The decision of UIDAI regarding engagement of ASA shall be final.

Examples of ASAs:

An agency such as National Payments Corporation of India (NPCI) that is currently mandated as the umbrella organisation to operate the retail payment systems in the country

DIT/NIC that provides connectivity solutions to various Central and State Government ministries / departments

Telecom carriers, depository bodies etc that provide related services to multiple organizations

ASA Readiness Stages

- Fill online application form – Any agency interested in becoming an ASA needs to apply online. UIDAI has an online workflow based application form for engaging with ASAs.
- Send signed contract and supporting documents to UIDAI – The ASA should send hardcopy of the signed contract along with required supporting documents to UIDAI. The online application would be approved by UIDAI upon receipt of the required documents.
- Establish leased line connectivity with CIDR – The ASA needs to draw secure leased line connectivity from its data centre to CIDR.
ASA should plan bandwidth, redundancy etc based on their business requirements.

- **Ensure process and technology compliance** – The ASA needs to setup necessary systems, processes, infrastructure etc. in compliance with UIDAI's standards and specifications. Compliance to various requirements needs to be confirmed to UIDAI through the online application form.

- **Obtain approvals from UIDAI** – UIDAI would approve an ASA’s application form when various compliance requirements are met. An ASA should engage with UIDAI during the process and provide required clarifications.

- **Carry out end-to-end testing** – Approval from UIDAI allows an ASA to carry out end-to-end testing of their connectivity with the CIDR. Before going live, it is highly recommended that an ASA works with an AUA to carry out end-to-end testing of the connectivity from devices to AUA to CIDR and reverse response communication. An ASA should also carry out load testing to ensure bandwidth adequacy. The ASA would also need to get the systems related to Aadhaar authentication audited by information systems auditors certified by a recognized body before going live.

- **Go-live** – An ASA can go-live after confirmation of adherence to all UIDAI's standards and specifications. UIDAI plans to manage the same through online workflow based application. In addition, an ASA can transmit authentication packet only after it engages with an AUA.

- **Engage with AUAs** – An ASA may enter into a formal contract with AUAs it supports. UIDAI has a set of proposed guidelines that may be included in the contract between an ASA and an AUA. However, the contract (and commercial terms, if any) between an ASA and an AUA is at the sole discretion of the signing parties and UIDAI does not have any responsibilities regarding same. Similarly, if an ASA provides any value added services to an AUA over and above Aadhaar authentication, UIDAI will not be party to any such services.

### Key ASA Responsibilities

- Ensure compliance of authentication related operations (processes, technology, security, etc.) to UIDAI's standards and specifications.

- Log and maintain details of all authentication transactions.

- Get its operations and systems related to Aadhaar Authentication audited as per UIDAI's specifications.

- Perform basic checks on the authentication input and forward it to CIDR

- Transmit the result of the authentication transaction received from CIDR to the AUA that has placed the request

- Inform UIDAI of the engagement/disengagement of AUAs that it serves

- Inform UIDAI of any misuse of Aadhaar data, authentication services, or any compromise of Aadhaar related data or systems.

### Mandatory Security Requirements

- ASA can connect to the CIDR only through a leased line.

- The meta data and the responses should be logged for audit purposes.

- Encrypted PID block and license keys that came as part of authentication packet should never be stored anywhere in its system.

- Network between AUA and ASA should be secure.

For further details, please visit [http://uidai.gov.in/auth](http://uidai.gov.in/auth)

For any clarifications, please contact Mr. Sameer Gupta, ADG, UIDAI at auth.ecosys@uidai.gov.in

Aadhaar Authentication Services
Aadhaar Seeding

Aadhaar seeding is a process by which UIDs of residents are included in the service delivery database of service providers for enabling Aadhaar based service delivery. Examples of seeding include linking Aadhaar numbers in the database of LPG companies against consumer IDs, linking Aadhaar numbers in core banking systems of Banks against Account numbers, linking Aadhaar numbers in NREGA database against Job Card numbers etc.

Why is Aadhaar Seeding Required?

Going forward, Aadhaar will form the basic, universal identity infrastructure over which government and other service providers across the country will be able to build their identity-based applications. These features in turn are expected to serve a developmental mandate to potentially achieve multiple transformational benefits of development and equitable growth through:

1. Proper identification leading to better targeting of development schemes provided by government, public sector and private sector
2. Ensuring that all fake, duplicate and ghost records are weeded out from databases so that leakages resulting from such records are avoided.
3. Increased reach and efficiency in delivering subsidized goods and services such as food, LPG, kerosene and fertilizer, banking and financial services, health, insurance, education etc.
4. No repeated KYC checks for residents

The above benefits may be achieved by leveraging Aadhaar authentication and Aadhaar based payments. To use these Aadhaar platforms, the Aadhaar number itself needs to be available along with the current unique identifier (Customer Id/ Beneficiary Id etc.) in service delivery databases. At the time of transaction, the mapped Aadhaar number in service delivery database needs to be sent for processing the request and therefore it is essential that Aadhaar seeding is performed.

Seeding Steps

Broadly, the following steps can be used for seeding Aadhaar numbers in databases:

1. **CAPTURE**: Capture Aadhaar number and Service Provider's ID (may also be referred to as department ID, program ID, customer ID, consumer ID, etc). Examples of such ID's are Ration card, MNREGS Job Card Number.

2. **VALIDATE**: Ensure that the Aadhaar KYR data and Service Provider's KYR data against the two ID's captured are compared and accepted as the same person.

3. **LINK**: Insert validated Aadhaar numbers in the Service Provider's database.

Digitization of department's beneficiary data should ideally be done before the start of “capture” step. If a department has paper-based records, digitization may be done either during “capture” or “validate” steps.

Key Considerations for Seeding

At the outset, it is to be noted that strategy for Aadhaar seeding is a combination of several sub-strategies and no one solution will apply to all cases.

Therefore it is essential that the seeding strategy for any given service delivery program is arrived at by considering various possible seeding methodologies while keeping in mind the beneficiary profile (senior citizens or pregnant women or children etc.), service characteristics (cash or kind, frequency etc.). While it is the responsibility of the service providers to seed their service delivery databases with Aadhaar, UIDAI will support by providing necessary tools, expertise, best practices and consulting advisory on request.
Broadly, seeding strategies could be inorganic (also referred to as Algorithmic / Batch / Top-down Seeding)

**Step 1: Capture**
1. Ensure Aadhaar KYR availability
   - State Resident Data Hub (SRDH) or equivalent
2. Ensure Department KYR availability
   - Digitize & Translate (to English) as necessary
3. User Access to both KYRs

**Step 2: Validate**
- System Assisted Validation (SRDH or equivalent)
  - Accept or Reject system recommended Aadhaar record for each given Department Beneficiary record
  - Auto-accept system selected Aadhaar record for each given Department Beneficiary record

**Step 3: Link**
1. Export validated Aadhaar no. and Department Beneficiary ID pairs in department database
2. Optionally export the Aadhaar KYR data also
3. Aadhaar Enabled database is ready for service delivery

or organic (also referred to as Bottom-up / Manual Seeding).

**Step 1: Capture**
1. Connect with residents using options such as:
   - Camps; Door-to-Door; resident touch-points, e.g. PDS shop, CSCs etc.; Self service mode of online/SMS
2. Collect UID numbers and program ID
   - Use Verhoeff Algorithm (for Aadhaar no. validation) or SRDH (to refer Aadhaar KYR)

**Step 2: Validate**
- Compare Aadhaar KYR to Program KYR using options such as:
  - Manual Verifier (and digitize data if not already done)
  - Demographic Authentication (AUA dependency)

**Step 3: Link**
Same as that for Inorganic Seeding

Precautions at the time of Capture
Some precautions to be exercised during data capture include:
1. Exact 12 digits of the UID should be captured. In case the capture is being done electronically, check-sum digit algorithm (or Verhoeff algorithm) should be applied at the point of capture to ensure that a valid 12-digit number is being collected.

2. Complete Department ID should be captured. Departments do not necessarily give a unique ID to all beneficiaries. For example, the LPG consumer number is a local ID, which is given by gas distributors (agencies) to its customers within the local geography and may only have 4 or 5 digits. While collecting LPG consumer number, the capturing agency or personnel should also capture the name of OMC and distributor (gas agency). A combination of OMC ID, distributor ID and local consumer ID would result in a unique consumer ID.

3. A lot of service provider IDs are family based IDs, such as the LPG consumer number, Ration card number etc. At the time of capture, name and Aadhaar numbers of all family members should be captured against such Family IDs.

**Multi-Methodology approach**
Often multiple methodologies will have to be adopted in parallel to enable effective seeding in the context of existing challenges with respect to data, timelines and operational realities. Multiple methodologies also provide a choice to residents to submit their Aadhaar numbers using a channel which suits them best. While some residents prefer self-service methodologies such as SMS, for some residents, assisted methodology such as a dedicated camp in the locality would work better.

Similarly, the validation methodology may also vary depending on the level of data digitization, stringency requirement by the department etc.

Aadhaar Seeding process should be designed as an ongoing mechanism and service providers should consider continuous monitoring and improvements in the seeding process.

For further details, please visit http://uidai.gov.in/auth
For any clarifications, please contact Mr. Sameer Gupta ADG, UIDAI at auth.ecosys@uidai.gov.in

Aadhaar Authentication Services
Financial inclusion is expected to be a key application of Aadhaar authentication. Adoption of Aadhaar and Aadhaar authentication in Indian banking system is expected to change the financial landscape of country.

To enable same, UIDAI has partnered with various stakeholders including RBI, NPCI, IBA and banks to develop two key platforms:

- **Aadhaar Payments Bridge (APB)** - A system that facilitates seamless transfer of all welfare scheme payments to beneficiary residents' Aadhaar Enabled Bank Account (AEBA)
- **Aadhaar Enabled Payment System (AEPS)** - A system that leverages Aadhaar online authentication and enables AEBAs to be operated in anytime-anywhere banking mode by the marginalized and financially excluded segments of society through microATMs

**Aadhaar Payments Bridge**

APB is a repository of Aadhaar number of residents and their primary bank account number used for receiving all social security and entitlement payments from various government agencies.

APB requires using Aadhaar number as the primary key for all entitlement payments. This would weed out all fakes and ghosts from the system and ensure that the benefits reach the intended beneficiaries.

This benefit has an even greater ramification as more and more social security programs are moving from in-kind to in-cash subsidies.

**APB Process Steps**

The key steps in posting payments via APB are:

1. Service delivery agency that needs to make payments to its beneficiaries (such as MGNREGA wages, scholarships disbursement, old age pension etc.) provides APB file containing details of Aadhaar number, welfare scheme reference number and the amount to be paid to its bank (called sponsor bank).
2. Sponsor bank adds bank IIN (Institute Identification Number provided by NPCI to participant banks) to the APB file and uploads onto NPCI server.
3. NPCI processes uploaded files, prepares beneficiary bank files and generates settlement file
4. Settlement file is posted to bank accounts with RBI
5. Destination banks can download the incoming files for credit processing after the settlement file has been processed.
Aadhaar Enabled Payment System

The Report of the Committee on Financial Inclusion chaired by Dr. C. Rangarajan, made two important observations:

A. Technology has to enable the banks to go where the customer is present, instead of the other way around.

B. Technology should allow interoperability among different systems adopted by different banks.

The Aadhaar Payment System is intended to address both the above issues.

AEPS empowers the marginalised and excluded segments to conduct financial transactions (Credit, Debit, Remittances, Balance Enquiry, etc) through microATMs deployed by Banks in their villages.

AEPS Process Steps

The key steps in doing transactions via AEPS are:

1. Resident provides his/her Aadhaar number, details of financial transaction sought and fingerprint impression at the microATM device.
2. Digitally signed and encrypted data packets are transferred via Bank Switch to NPCI to UIDAI.
3. UIDAI processes the authentication request and communicates the outcome in form of Yes/No.
4. If the authentication response is Yes, bank carries out the required authorization process and advises microATM on suitable next steps.

Benefits to Various Stakeholders

Residents

- Obviates need for multiple bank accounts for different schemes
- Faster channel for receiving all welfare payments without any middle-men
- Access to microATM in villages saves bank trips, thus reducing opportunity and access costs
- Will help in more usage of formal banking system for managing savings and borrowing

Online and interoperable architecture of AEPS ensures anytime-anywhere access of bank accounts which can be a boon especially for the migrant population estimated to be 100 million

- Empowerment of individuals especially women

Government Departments

- Use of Aadhaar as primary key eliminates ghost beneficiaries and leads to better targeting
- Sub-serves goal of furthering Financial Inclusion by processing government disbursements through Aadhaar number
- Reduces time and cost in payment processing
- Provide electronic audit trail and end-to-end visibility for all payments

Banks

- Reduces the credit and operational risks in the branchless banking model
- Enables Banks to rely on BCs to reach the unbanked population, eliminating the need for a physical bank branch or ATM's in remote areas
- Will provide an impetus to electronic payments and thus reduce cash management costs
- Different financial products through microATMs can be an additional source of revenue for banks and for the BC model

RBI

- Sub-serves goal of furthering Financial Inclusion by processing government disbursements through Aadhaar number
- Promotes electronification of retail payments through a secure mechanism

Prerequisites for APB & AEPS

- Aadhaar – welfare scheme number mapping
- Aadhaar number seeding in computerized databases if any
- Opening of AEBA

For further details, please visit http://uidai.gov.in/auth
For any clarifications, please contact Mr. Rajesh Bansal, ADG, UIDAI at rajeshbansal@uidai.gov.in

Aadhaar Authentication Services
Authentication Devices

Authentication Devices

Aadhaar authentication is initiated through authentication devices. Authentication devices perform the following key functions:

- Collect PID from Aadhaar holders
- Perform basic checks on the information collected for completeness and compliance
- Prepare the authentication data packet for transmission as per Aadhaar authentication APIs
- Transmit the authentication packets for authentication
- Receive the authentication results along with instructions for next steps if any

Authentication devices are deployed by the AUA, Sub AUA or their agents. The connectivity from devices to AUA/ Sub AUA server is also provisioned by the AUA/ Sub AUA.

Device Specifications

Authentication devices are expected to be used for a variety of purposes and would need to be specific to every AUA’s requirements. To cater to the varied application needs of different AUAs, while ensuring authentication packets received from AUAs are standard and secure, UIDAI has adopted an API based approach for authentication application.

For the hardware component, demographic and OTP based authentication 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 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 – http://stqc.gov.in/content/bio-metric-devices-testing-and-certification

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.

Some possible form factors in which biometric authentication devices may be deployed include:

- Hand-Held / PoS Device such as MicroATMs, attendance devices
- USB device connected to PC
- Mobile phone with biometric sensor
- Kiosks such as ATMs, MNREGA job request kiosks

AUAs are expected to select form factor based on their service delivery and deployment needs.

Some AUAs may also need to specify suitability to specific environmental conditions such as, hot/cold desert, high humidity areas etc.

Based on network availability in locations where devices are deployed, AUAs may also consider opting for solutions such as dual SIM, external antennas etc.

Application Components on Devices

- Authentication application – AUAs should develop authentication application based on its business needs and UIDAI’s authentication API.

- Best Finger Detection (BFD) application – Success of biometric authentication is dependent on the quality of biometric captured in the authentication request. The quality varies across different fingers of a resident, amount of pressure applied etc. To ensure that a resident is
on-boarded to the concept of biometric authentication and is aware of which fingers are best suited for biometric authentication, UIDAI has developed a protocol called BFD. If an AUA opts for biometric authentication, it should ensure that the BFD application, as per the BFD API published, is deployed on the devices.

- **OTP application** – If an AUA opts for Aadhaar-based OTP authentication, the AUA should build a module for initiating OTP request and integrate the same with its service delivery application. The API for developing OTP request application is available on UIDAI’s website. As a backup option, the AUA may also guide residents to generate OTP through UIDAI’s portal, UIDAI’s contact centre or USSD through resident’s registered mobile phone.

- **Exception handling provisions** – The device application should have provisions to service genuine residents who may be falsely rejected during biometric authentication. Also, there should be measures to continue service delivery in case of other technological limitations such as network non-availability, device breakdown etc. There should be no denial of service to residents due to technology limitations. The exception handling mechanisms should be backed up by non-repudiable features to log and track requests handled through exception handling mechanism to prevent any fraud attempts.

**Authentication Environment**

Authentication devices could be operator-assisted or self-operated. Similarly, the environment in which the authentication devices are deployed could either be managed/monitored by AUA or unmanaged/not-monitored. While devices in operator-assisted, AUA managed environment would provide highest level of trust, it may not be practical for all authentication purposes.

AUA should make a comprehensive risk assessment while considering the environment factors before finalizing authentication type, security and audit measures, fraud monitoring requirements etc.

**Device Operator Training**

A large number of authentication devices, especially those initiating biometric authentication requests, are expected to be operator-assisted devices. AUAs should ensure that operators are adequately trained to carry out Aadhaar authentication transactions and also to handle resident queries appropriately.

Some key areas that should be part of operators’ training include:

- 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 and ensuring no denial of service to residents due to technology limitations
- Communicating appropriately with residents
- Fraud monitoring & fraud reporting mechanisms
- Basic troubleshooting steps and contact details of AUA’s device/application support team

**Mandatory Security Requirements**

- 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 short 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.

For further details, please visit http://uidai.gov.in/auth
For any clarifications, please contact Mr. Yashwant Kumar, ADG, UIDAI at auth.ecosys@uidai.gov.in

Aadhaar Authentication Services
For Residents

1. **What is Aadhaar authentication?**
   Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic and/or biometrics and/or OTP) is 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 a “yes/no”. No personal identity information is returned as part of the response.

2. **When do I need to authenticate?**
   Various service providers, such as PDS, NREGA, banks, are expected to link Aadhaar authentication to their services. Residents would need to authenticate either at the time of subscribing to the service or at the time of availing service delivery, as required by the service providers.

3. **What are the benefits of Aadhaar authentication?**
   The purpose of Authentication is to enable residents to prove their identity and for service providers to confirm that the residents are ‘who they claim they are’ in order to provide services and benefits.

4. **From where can I authenticate?**
   Authentication requests will be initiated at the point of service delivery by agencies using Aadhaar authentication. Examples include FPS shops, NREGA centres, bank terminals etc. These centres may be “assisted” (an operator handles the device) or “self-service” (kiosks, mobile phones, Internet terminals, etc.).

5. **How can I authenticate?**
   To authenticate, residents should provide their Aadhaar number & other authentication attributes as requested by the service provider. The request is then sent to UIDAI’s CIDR for authentication.

6. **What does online authentication mean?**
   Online authentication implies that data submitted is matched against data available in a central database (vs. offline authentication, where data submitted is matched against data stored locally such as smart card).

7. **How is Aadhaar authentication different from smart card authentication?**
   In Aadhaar authentication, Aadhaar number of a resident & the data to be authenticated is sent online to UIDAI’s CIDR for matching against data present in CIDR.
   In smart card authentication, the data/biometric is checked against data stored in the smart card.
   Aadhaar online authentication will have certain distinct advantages over offline authentication in terms of being more cost effective, more secure and allowing portability.

8. **Through Aadhaar authentication, can someone find out my personal information?**
   No. CIDR only returns “Yes/No” after matching the data submitted along with the Aadhaar number.

9. **What all data can be authenticated / verified with UIDAI?**
   UIDAI provides demographic data verification & biometric authentication. Demographic data includes name, address, gender, age/DOB, mobile number, email address. Biometric authentication can be done through fingerprints or iris. In addition, UIDAI also provides OTP based authentication.

10. **Is there a mechanism to notify the residents when an authentication occurs against their Aadhaar number?**
    UIDAI has an sms and email based notification mechanism. Through this mechanism, every time CIDR receives an authentication request against an Aadhaar number, a notification will be sent to the registered mobile / email address.

11. **Can I choose whether or not to receive notification when someone authenticates me?**
    For biometric & OTP authentication, notification will necessarily be sent to the registered mobile and email address.
    For demographic data verification, residents can choose whether or not to receive notifications.
12. I received an authentication notification even though I did not authenticate myself. Whom do I approach?

The authentication notification will contain the name of the service delivery agency through which authentication request was received. Residents are advised to approach the respective service delivery agency.

13. What if my authentication request gets rejected even though I provide my biometric/demographic details with my Aadhaar number?

If biometric authentication fails, residents can retry multiple times with different fingers, appropriate pressure and cleaning the sensor/fingers.

If biometric authentication fails over a period of time, resident go for Best Finger Detection (BFD) which will guide on the next steps.

If demographic authentication fails, retry with correct data provided at the time of enrolment & as printed in resident’s Aadhaar letter.

14. What is Best Finger Detection (BFD)?

Success of biometric authentication depends on the quality of biometric captured in the authentication request and enrolment. The quality varies across fingers, amount of pressure applied etc. To educate residents on their suitable fingers for biometric authentication, UIDAI has developed the BFD protocol.

BFD application requires a resident to provide biometric authentication through each of the ten fingers one-by-one. A request with all ten fingerprints is sent to CIDR, which in turn returns a response indicating which fingers are best suited for Aadhaar biometric authentication.

Based on the fingerprint quality analysis, the resident may also be advised to update their biometrics with CIDR. For further details, residents can contact UIDAI’s contact centre.

15. Do I need to undergo BFD before every biometric authentication?

No. BFD or resident on-boarding is expected to be a one-time exercise, preferably before a resident does first biometric authentication.

16. Where can I get BFD done?

Every AUA is expected to deploy BFD application on their devices, which would be an integral part of the authentication device/application.

17. What if I authenticate with a finger other than the “best” finger identified by the BFD tool?

BFD helps improve chances of successful authentication with minimal number of attempts. If a resident authenticates if a finger other than the “best” finger, the authentication packet will still be processed. If the authentication fails, resident may try with another finger.

18. Will I be denied my entitlements (ration, NREGA job etc.) if my authentication request is rejected?

UIDAI and the supporting ecosystem recognize that Aadhaar authentication is subject to technological and biometric limitations such as false accepts, false rejects, network availability etc. To counter the same, the service providers will have alternate processes to identify/authenticate their beneficiaries/customers.

Residents should not be denied entitlements due to technological or biometric limitations.

19. How will I authenticate if my fingerprints are worn out / I have no fingers?

Service providers are advised to deploy alternate authentication mechanisms including Aadhaar OTP to handle such issues.

20. How do I request for OTP?

OTP can be requested through service providers’ application requiring OTP authentication, mobile number registered with CIDR, Aadhaar portal or Aadhaar contact centre.

OTP will always be delivered to registered mobile and/or email.

21. I do not have mobile / email. How will OTP be delivered to me?

In the context of Aadhaar, usage of OTP adds the factor of “possession of mobile/email address” as a way to strengthen the authentication. Hence OTP will not be available as an option for residents who have not registered their mobile number or email with Aadhaar system.
For AUAs & ASAs

1. **What are the expected benefits of Aadhaar authentication? How to use Aadhaar authentication as part of service delivery?**
   
   Some of the expected benefits are:
   - Establishing identity for purposes such as adding new beneficiaries, confirming genuine beneficiary before service delivery, financial transactions etc.
   - Enabling demand-driven, portable service delivery by providing anywhere anytime real-time authentication
   - Access to relevant MIS and empowerment of beneficiary
   - Improving efficiency & transparency in service delivery by enabling tracking of end-to-end service delivery process, improving accountability and vigilance etc.
   - Access control to restricted areas such as airports, hotels, high security buildings etc.
   
   Aadhaar authentication may be used at various points in service delivery when there is a need to authenticate beneficiaries, officials or other members of service delivery chain.

2. **How can Aadhaar authentication be used for cleaning up database(s)?**
   
   Aadhaar fundamentally provide two values – uniqueness and online authentication. Uniqueness attribute can be used to eliminate ghosts & duplicates, if any, from databases. Online authentication for demographic data such as name, address, age/DoB, mobile number and email address can be used for keeping database up to date and clean.

3. **How can an AUA use Aadhaar authentication services to seed Aadhaar in their database?**
   
   Before adding Aadhaar to its database, an AUA can verify the correctness of the Aadhaar number through authentication.

4. **Is resident involvement mandatory for every Aadhaar authentication?**
   
   Resident involvement is not necessary for demographic authentication, wherein an AUA can verify demographic attributes available in AUAs' database. However, for biometric and OTP authentication, resident involvement is necessary for every authentication transaction.

5. **Do the names/addresses of beneficiaries/customers in AUA database need to be spelled same as that in CIDR for verification?**
   
   Not necessary. Aadhaar authentication supports exact match and partial match. Partial match implies that based on a threshold that an AUA sets, name “Ram Kumar” can be authenticated as “R Kumar” OR “Ram K”. For partial match, at least spelling of one word should match exactly. Similarly, for address, the verification can be either entire address verification or partial at state, district, pin code, village / town/city, locality, house number level.

6. **What all authentication factors is UIDAI supporting?**
   
   Besides demographic data verification, UIDAI offers following factors of authentication for cases where it is required to prove “who you say you are”:
   - Who you are (inherence factor) – biometrics
   - What you have (possession of mobile) – OTP

7. **Can an AUA use one authentication factor from UIDAI & another one from itself?**
   
   Yes. UIDAI advocates federated authentication system wherein, the AUAs are encouraged to use Aadhaar Authentication in conjunction with the AUA’s existing authentication system.
   
   Aadhaar authentication will supplement & work in conjunction with existing authentication systems to strengthen the overall authentication rather than replace existing authentication systems.

8. **Can Aadhaar authentication be combined with ATM/card based authentication? If yes, how?**
   
   Yes. An AUA is free to combine multiple authentication factors for strengthening the authentication services / fulfil other service/business/regulatory needs.
9. How many fingers should be used for authentication?

One or more fingers can be used for an authentication transaction.

10. What does an AUA need to do to use Aadhaar authentication?

Key steps to be followed include:
- Identify business / service delivery needs and select appropriate authentication types
- Fill online application form
- Engage with ASA(s)
- Send signed contract and supporting documents to UIDAI
- Ensure process and technology compliance
- Plan device deployment
- Obtain approvals from UIDAI
- Carry out end-to-end testing
- Go-live

11. Is it necessary for an agency seeking to utilize Aadhaar authentication for its service delivery to have direct agreement with UIDAI?

Aadhaar authentication ecosystem has provision wherein any agency seeking to use Aadhaar authentication of its customers/associates etc for service delivery can engage with an existing AUA. Such agencies which enter into agreements with AUA are defined as Sub-AUA. Any agency wanting to become an AUA needs to have an agreement with UIDAI directly.

12. What is the extent of process & technology re-engineering required for using Aadhaar authentication?

To reap maximum benefits from Aadhaar authentication, AUAs may re-engineer some of their processes and technology. AUAs could use Aadhaar authentication to not only verify their beneficiaries / customers but also improve efficiencies in their entire supply chain.

Adoption of Aadhaar authentication may also provide an opportunity to various service delivery agencies to review and improve their service delivery model.

At the minimum, AUAs would need to identify points in their service delivery where Aadhaar authentication may be integrated and then ensure the technology and processes are integrated for doing the same.

The details of technology re-engineering required are available on technical FAQs, API & other technical documents present on UIDAI's website http://uidai.gov.in/.

13. Can someone help me with the process & technology re-engineering?

UIDAI has empanelled certain consulting and software development companies who may be roped in for the required support.

AUAs are also free to either use in-house skill set or carry out their own tendering and procurement process for hiring services of entities that may help with technology re-engineering.

14. Will UIDAI provide the client application required for doing authentication?

UIDAI provides API documents and reference implementations. AUAs need to develop client application based on their requirements related to service delivery, authentication interface, probable devices etc.

15. Are there any specific application components that need to be included in authentication client application?

Besides the authentication application, which is based on AUA's business needs and UIDAI's authentication API, the authentication devices should have following applications:
- Best Finger Detection (BFD) application
- OTP application
- Exception handling provisions

16. What is OTP application?

If an AUA opts for Aadhaar-based OTP authentication, the AUA should build a module for initiating OTP request and integrate the same with its service delivery application. The API for developing OTP request application is available on UIDAI's website.
17. What are exception handling provisions and why are they required?

The device application should have provisions to service genuine residents who may be falsely rejected during biometric authentication. Also, there should be measures to continue service delivery in case of other technological limitations such as network non-availability, device breakdown etc. There should be no denial of service to residents due to technology limitations.

18. What kind of devices need to be used?

An AUA can choose a suitable device form & factor depending on its deployment environment and other service delivery / business need. For biometric authentication, AUA would need to adhere to sensor and extractor SDK specifications provided by UIDAI. These sensors and extractors can be integrated with device form and factor suitable to AUA.

19. Would UIDAI be certifying devices? If yes, how?

Certification is required only for the sensor and extractor combinations required for biometric authentication. Overall devices will not be certified. The certification will be done by a STQC. The certification process would be similar to that of enrolment biometric devices. The details are on http://www.stqc.gov.in/.

20. Does each device need to be registered with UIDAI / CIDR?

As part of public devices and currently published authentication specification, registering each device is not required. In the future, as specifications change, this may be required. UIDAI will publish updated specifications and processes.

21. Is there any certification mechanism for the authentication device operators?

Not as of now. Training & certification of operators/devices depends on AUAs business model and rules.

In case an AUA opts for biometric authentication, some key areas that should be part of operators' training include:

- 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 and ensuring no denial of service to residents due to technology limitations
- Fraud monitoring & fraud reporting mechanisms
- Basic troubleshooting steps and contact details of AUA's device/application support team

22. Do the operators need to get registered with UIDAI / CIDR?

Not as of now. AUAs are expected to manage all partners and users within their network for conducting transactions.

23. How can devices be connected to servers for authentication? Any leased line required?

Remote devices should be able to send authentication request to AUA servers over various types of networks – mobile network, PSTN, broadband. UIDAI mandates a leased line only between ASA and CIDR.

24. What is the expected turnaround time for authentication response?

Under normal circumstances (depending on the choice of network by the AUA), the expected turnaround time is 1 second to 10 seconds.

25. How to carry out authentication if network connection is down?

For cases where connectivity is intermittent or connectivity is a little distance away, UIDAI has a solution called “buffered” authentication.

26. What is buffered authentication?

Buffered authentication is a type of online authentication where requests are queued up at the device for up to 24 hours and sent to CIDR when connectivity is restored. Buffered
authentication may be used in situations where connectivity is intermittent or connectivity is a little distance away.

27. What is resident on-boarding process?

One of the known limitations of biometric technology is false rejections. To minimize the same and provide residents an opportunity to understand their biometrics better before doing authentication, UIDAI proposes a resident on-boarding process to be implemented by AUAs. This will also help manage resident expectations and provide guidance to AUAs for exception handling requirements, if any.

As part of this process, when resident approaches an AUA for biometric authentication for the first time, BFD is carried out and resident is advised of this best finger(s) for authenticating. If required, a resident may also be advised to approach an Aadhaar updation centre to update his/her biometrics.

28. When should BFD be done? How will an operator know when to initiate BFD application?

BFD or resident on-boarding is expected to be a one-time exercise, preferably before a resident does first biometric authentication. BFD application should be integrated with the overall service delivery application and should be initiated based on a certain API error code returned by CIDR.

29. Does an AUA need to set up dedicated centres for BFD / Resident on-boarding?

No, BFD / resident on-boarding may be carried out through the standard service delivery authentication devices that an AUA deploys. BFD is done through a single fingerprint scanner. Other details of BFD are available in the BFD API document.

30. Who are the ASAs that an AUA can approach for carrying out Aadhaar authentication?

ASAs are entities with secured lease line connectivity with UIDAI CIDR. The list of approved ASAs will be available online. An AUA can choose to engage with any of the approved ASAs. An AUA may become its own ASA as well by establishing leased line and completing rest of the process-technology integration.

31. Can ASAs charge money for enabling Aadhaar authentication?

Yes, ASAs can charge for the services they offer to AUAs. By enabling several ASAs and also allowing AUAs to connect directly, UIDAI will ensure choice and healthy competition.

32. How can an entity become an ASA?

The qualification criteria for becoming an ASA are published on UIDAI's website. Any entity fulfilling the criteria and interested in becoming an ASA needs to do the following:

- Fill online application form
- Send signed contract and supporting documents to UIDAI
- Establish leased line connectivity with CIDR
- Ensure process and technology compliance
- Obtain approvals from UIDAI
- Carry out end-to-end testing
- Engage with AUAs

33. Who all can connect to “Public authentication URL” offered by UIDAI?

This is provided only for testing purposes. This is not expected to be used for production. The URL is http://auth.uidai.gov.in/.

34. What kind of contracts, obligations do AUAs/ASAs need to sign/understand?

Both AUAs and ASAs need to sign contracts with UIDAI. The contract between AUA and ASA is the discretion of signing parties. UIDAI has a set of proposed guidelines that may be included in the contract between an ASA and an AUA. However, the contract (and commercial terms, if any) between an ASA and an AUA is at the sole discretion of the signing parties and UIDAI does not have any responsibilities regarding same. Similarly, if an ASA provides any value added services to an AUA over and above Aadhaar authentication, UIDAI will not be party to any such services.
Financial Inclusion

1. Will an Aadhaar Enabled Bank Account (AEBA) be opened with every issue of an Aadhaar number?

AEBA will be opened for every resident who chooses to do so at the time of enrolment.

2. Can the existing bank accounts also be linked to Aadhaar?

Customers can link their existing bank accounts to Aadhaar by contacting their bank. All banks are in the process of implementing Aadhaar-linkage processes.

3. How will an Aadhaar enabled bank account help a resident that already has a bank account?

It is envisaged that disbursement Electronic Benefit Transfer (EBT) payments and Direct Transfer of Subsidy (DTS) payments will be transferred into Aadhaar-enabled accounts. This includes social security benefits like pensions, scholarships, MGNREGS wages, LPG subsidy, Fertilizer subsidy, etc.

4. What is an Aadhaar Enabled Bank Account (AEBA)?

AEBA is a bank account linked to Aadhaar number of the resident that allows transactions on the basis of resident's Aadhaar number.

5. What is the Aadhaar-Enabled Payments System (AEPS)?

The AEPS is an interoperable network of microATMs that is operated by NPCI. It will enable the following interoperable transactions:

1. Cash withdrawal
2. Cash deposit
3. Balance enquiry
4. Remittance

Further details are available at http://www.npci.org.in/AEPSOverview.aspx

6. What are micro-ATMs? How will they work in the Aadhaar system?

Micro-ATMs are compact payment devices that are operated by a BC or BC sub-agent appointed by Banks. The micro-ATM standards are published at http://uidai.gov.in. Micro-ATMs will enable all the banking transactions allowed in AEPS.

7. What is the Aadhaar Payments Bridge (APB)?

APB is a backend payments processing platform that allows Government agencies to transfer funds into AEBA using only an Aadhaar number, and the amount to be transferred.

8. How can an agency use APB for transferring funds to be disbursed to their beneficiaries?

The key requirements for using APB are:

a. Seed Aadhaar in their beneficiary database. This requires mapping Aadhaar number to the welfare scheme number such as MGNREGA job card number.

b. Ask their bank to work with NPCI and obtain Institutional Identification Number (IIN) and integrate APB with their system.

c. Create APB file containing Aadhaar number, bank IIN, amount and welfare scheme reference number and provide to their bank.

9. Does a service delivery agency need to sign any contract / engage with any specific organization(s) to post payments via APB?

The service delivery agency needs to engage with their bank to avail of APB. The bank in turn gets the agency registered with NPCI.

10. Does a service delivery agency necessarily need to become AUA to use APB / AEBA / AEPS?

Service delivery agency need not become AUA to use APB / AEBA / AEPS. The bank that will offer AEPS to its customers would need to become an AUA / sub-AUA of UIDAI.

11. What does a bank need to do to avail APB/AEPS?

To become a member of APB, banks need to work with NPCI. To use AEPS, banks need to become AUA / sub-AUA of UIDAI as well as work with NPCI for overall integration.

Aadhaar Authentication Services
List of Documents Available on UIDAI’s Website

Technical Documents
- Aadhaar Authentication Security Model
- Aadhaar Authentication API Specification
- Aadhaar Best Finger Detection API Specification
- Aadhaar OTP Request API Specification
- Biometric Devices Specifications for Aadhaar Authentication
- ASA Handbook
- Guidelines for Handling API Error codes
- Standards and Specifications Document
- Technology FAQs

Other Documents
- Aadhaar Strategy Document
- Aadhaar Authentication Framework
- Aadhaar Authentication Operating Model
- UIDAI-ASA Agreement Template
- UIDAI-AUA Agreement Template
- Guidelines for AUA-ASA Agreement
- Guidelines for AUA-Sub AUA Agreement
- Aadhaar Seeding Strategy
- White Paper on Aadhaar Enabled Service Delivery
- FAQs for Residents and AUAs/ASAs

Financial Inclusion
- AEPS Operating Procedures
- AEPS On-boarding Document
- AEPS Interface Specification
- APB Operating procedures
- APB On-boarding Document
- MicroATM Standards

Contact Details
- Support for AUA/ASA technical & application integration: Request may be sent for membership to Google group aadhaarauth https://groups.google.com/forum/#!forum/aadhaarauth
- Technical Operations Support: Email ID: authsupport@uidai.gov.in; Phone No: 0120-4405610
- Authentication Ecosystem Management Support: Email ID: auth.ecosys@uidai.gov.in
- Financial Inclusion Support: rajeshbansal@uidai.gov.in
- Aadhaar Payment Bridge Support: apbs@npci.org.in
- Aadhaar Enabled Payment System Support: aeps@npci.org.in