
# Aadhaar Authentication Document for Delivery of Services

Version 1.0


Unique Identification Authority of India

(UIDAI)

# Contents

# 1. Introduction

The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. With the Aadhaar enrolment already taking place at many locations across the country, the downstream services and applications of the Unique Identification (Aadhaar) number shall need to be formulated and operationalised. The UIDAI provides online authentication using demographic and biometric data. The UID (Aadhaar) Number, which uniquely identifies a resident, will give individuals the means to clearly establish their identity to public and private agencies across the country.

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.

Various service providers have been using Smart Cards for offline validation of the beneficiary at the point of service delivery. The details of beneficiary including biometrics are stored in the smart card and verified locally at the time of service delivery. The cost of issue of Smart Card and maintenance is high. Since an Aadhaar holder may easily establish his identity before any service provider through the process of on-line Aadhaar authentication, the use of Smart Cards for the purpose of off-line verification of beneficiary's identity may not be necessary, especially in view of the fact that internet connectivity is increasingly available even in remote areas for online authentication

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data 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 UIDAI confirms either proof of identity or verifies the information provided by the resident based on the data available in the CIDR 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.

The document details the Authentication services offered by UIDAI. Aadhaar authentication provides several ways in which a resident can authenticate themselves using the system. At a high level, authentication can be 'Demographic Matching and/or 'Biometric/ OTP Matching. But, in all forms of authentication the Aadhaar Number needs to be submitted so that this operation is reduced to a 1:1 match.

Since Dec 2012 up to Jan 2016, over 35 crore Aadhaar holders have carried out more than 127 crore authentication transactions to establish their credentials for delivery of service. Up to 16th December 2015, over 3.5 crore Aadhaar holders have provided their eKYC details to various service providers.

## 2. Aadhaar Authentication

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data 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.

Authentication shall enable residents to prove their identity based on the demographic and/ or biometric information captured during enrolment, thus making the process of identification convenient and accurate. Aadhaar Authentication shall make life simpler for residents and eliminate the distress and inconvenience in establishing their identity for availing services. Through Aadhaar Authentication, more residents shall be able to prove their identity and thereby become eligible to benefit from Government schemes and subsidies. Aadhaar Authentication shall help AUAs in delivering services to eligible beneficiaries based on establishing their identity, thus improving efficiency and transparency in service delivery to the common man.

Aadhaar is a permanent and non-revocable identity as opposed to currently existing identity systems which are based on local, revocable credentials. Hence, AUAs are encouraged to use Aadhaar Authentication in conjunction with the AUA's existing authentication process so as to strengthen their authentication process. Aadhaar Authentication should be perceived as a mechanism to strengthen the current authentication process followed by AUAs to authenticate residents/ beneficiaries and enhance the level of identity authentication assurance while providing convenience to the resident.

It should be understood that the Aadhaar authentication system is not a 100 percent accurate system, irrespective of the kind of attributes selected for authentication. In cases where Authentication Device operator has sufficient reason to conclude that the outcome of an Aadhaar authentication result is not accurate, the operator may explore alternate mechanisms, including verification of Proof of Identity/ Proof of Address documents for establishing the identity of a genuine resident. The AUA shall put in place practices and procedures for handling exceptions so as to deliver services to all genuine beneficiaries.

Aadhaar Authentication supports:

1. Demographic Matching
2. Biometric Matching and
3. Additional features such as One-Time-Password (OTP)

***Demographic Matching***

Demographic matching refers to the usage of Aadhaar Authentication system by AUAs for matching Aadhaar number and the demographic attributes (name, address, date of

birth, gender, etc. as per API specifications) of a resident in the CIDR with the data in the AUA's database or with demographic data submitted at the point of authentication.

For example, demographic matching could be used by:

- Banks for automated KYC checking
- Any government welfare scheme for eliminating fake and duplicate identities in their databases
- Telecom service providers for address verification
- Private institutions/ banks for date of birth verification

***Biometric Matching***

Biometric Matching refers to the usage of Aadhaar Authentication for matching the biometric attributes of a resident in the CIDR to the biometric data submitted by the resident on an authentication device.

For example, biometric matching could be used by:

- Banks for establishing identity of customers before starting a new bank account
- Telecom service providers before issuing a new mobile connection
- Any organization for attendance tracking

***Matching using any other factors such as One-Time-Password (OTP)***

In this case, an OTP is sent to the registered mobile phone number of the resident seeking Aadhaar Authentication. The OTP shall have a limited validity. The resident shall provide this OTP during authentication and the same shall be matched with the OTP at the CIDR.

For example: OTP based authentication could be used by

- Banks for authenticating customers during internet banking transaction

- E-commerce companies before completing a cash-on-delivery transaction

## 3. Uses of Aadhaar Authentication

The authentication service provided by UIDAI can be used by the AUA or the Sub AUA for the following purposes (these are only indicative and is not an exhaustive list):

1. Establishing Identity during Know Your Citizen (KYC) or during service delivery
2. Elimination of fake and duplicate identities in existing application and database
3. Improving efficiency & transparency of service delivery
4. Eliminating the need of Smart Card for identification of beneficiary for service delivery

***Establishing Identity during KYC or during service delivery***

Biometric confirmation to add new users / customers – Aadhaar is envisaged to provide identity to the unreached & marginalized. Aadhaar-based biometric authentication would allow such residents access to critical services such as banking & telecom. This usage will also help manage cases of impersonation / false identity in services such as obtaining new phone connection, credit cards etc. Various financial institutions like banks could use Aadhaar authentication to establish the identity of customers before starting a bank account for new customers through biometric matching. Similarly, telecom service providers could use Aadhaar authentication to authenticate customers and establish their real identity, before issuing new connections (SIM cards) and duplicate SIM cards.

Confirming Beneficiary – Various social sector programs where beneficiaries need to be confirmed before delivery of the service are expected to be the most common users of the authentication service. Examples of some such usages include food grain delivery to PDS beneficiaries, health service delivery to RSBY beneficiaries, registering job applications by NREGA beneficiaries etc. This usage would ensure that services are delivered to the right beneficiaries.

Attendance tracking – Another key usage of authentication would be attendance tracking for programs such as SSA (for students & teachers), NREGA where wages / outlay is linked to actual number of days the beneficiary reports for the program etc.

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.

Various internet, social networking and e-commerce related websites could also use Aadhaar Authentication to authenticate customers/ subscribers whenever it is required to establish the real identity of the person who subscribes or does a transaction.

Besides standard security related requirements such as entry to airports, hotels etc., new usages of Aadhaar-based authentication could be as identity proofs in various examinations (such as medical, engineering entrance etc.) where a large number of cases of impersonation are reported every year.

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 date of birth can also be verified through Aadhaar authentication.

***Elimination of fake and duplicate identities in existing application and database***

During enrolment, de-duplication is done (using biometrics) to issue Aadhaar numbers to residents and hence, the Aadhaar numbers are unique. Hence, when Aadhaar numbers are seeded into existing databases, it can help in elimination of fake and duplicate identities, thereby cleansing the database. For e.g. Public Distribution System (PDS) databases can be cleansed of all fake and duplicate identities by seeding Aadhaar number into it, as each person will have only one Aadhaar number.

Once the Aadhaar numbers are seeded into the database, one-time authentication of new beneficiaries/ customers can be done during their enrolment into the respective programs/ schemes and this shall prevent fake and duplicate identities from entering existing databases.

***Improving Efficiency & Transparency in Service Delivery***

Track end-to-end service delivery process – At a transaction level, Aadhaar-based authentication if implemented across the service delivery process / supply chain will help curb leakages and diversions, and help identify bottlenecks in delivery. Some such applications would be:

- In PDS, track food grain as it is exchanged between PDS intermediaries

- In NREGA, track job application, job assignment, attendance, muster rolls & wage payments
- Link JSY, ICDS and SSA to ensure health and education for every child

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 & favorable to the beneficiaries. Some such benefits would include:

- PDS beneficiary need not be tied to one fair price shop (FPS) and can withdraw rations anywhere
- Migrants can access their PDS rations after leaving their village
- Children of migrants can continue school education in the new place as well

Strengthen existing accountability / vigilance procedures – Although various service delivery processes have vigilance groups and monitoring systems in place, the government and the public have no means of verifying whether vigilance checks and inspections were carried out, and who is accountable for delays and leakages. Aadhaar-based authentication of the vigilance officers/inspectors/auditors combined with time stamping & GPS tracking can strengthen the vigilance & accountability activities. Some examples of this usage include:

- Audits during food grain movement in the PDS program to control diversions
- Engineer/Gram Rozgar Sewak activities in NREGA
- Social audits in mid-day meal program, NREGA etc.

Access to relevant MIS and empowerment of beneficiary – Since Aadhaar will be able to uniquely identify each beneficiary, they would be able to check their entitlements, timeline by when services will be delivered to them, log grievances related to poor service / denial of service etc. without depending on any middle-man. The same can be enabled through self-service kiosks (already being piloted by NRGEA), mobile phones, call centers etc.

***Eliminating the need of Smart Card for identification of beneficiary for service delivery***

Smart cards are being used by various service providers for identification of the beneficiary at the point of service delivery. In the smart card system, the beneficiary’s personal details, biometrics and other service related details are stored locally in the smart card. The smart cards issued to the beneficiary are validated using point of sale terminal installed at the service delivery point.

The details of the beneficiary stored in the smart card are locally verified using PoS terminal at service delivery point. As the smart card system is localized system, proper de-duplication of beneficiary is not possible. The smart cards are also required to be periodically updated for changes in the personal details or entitlement of the beneficiary and thus have a life cycle. Smart cards are also prone to damage due to multiple uses and mishandling. Hence the cost of issue and management of smart cards is very high. However, the smart card offers offline authentication of the beneficiary and the system does not require online connectivity to the server/database.

Aadhaar Authentication is an economical, online authentication service that offers distinct advantages over other offline authentication modes like smart card in terms of being cost-effective, more secure and allowing national portability. In case of biometric authentication, any of the 10 fingers or any of the 2 Iris images of the beneficiaries can be utilized for establishing identity of the resident. In cases, where the fingers/Iris of the resident are damaged /cannot be used, Aadhaar system allows OTP for authentication. Aadhaar is thus inclusive in nature and handles such biometric exceptional cases.

Various organisations can on-board as Authentication User Agency (AUA), seed the Aadhaar number in their beneficiary database and provide services effectively and efficiently through the process of Aadhaar Authentication. This process is unique and robust enough to uniquely identify the beneficiary's and clean existing databases by eliminating fake / duplicate identities in databases. It is economical and convenient, both for the beneficiary as well as the organization that is providing the benefits. Since an Aadhaar holder may easily establish his identity before any service provider through the process of on-line authentication, the use of Smart Cards for the purpose of off-line verification of beneficiary's identity may not be necessary, especially in view of the fact that internet connectivity is increasingly available even in remote areas for online authentication.

Further, the cost involved in the issue of Smart Cards is very high and would also involve cost of updation of data and cost of equipment / terminal for offline verification of the Smart Card. Whereas, the biometric devices / units used by Aadhaar System for online authentication are STQC certified and the present cost of biometric device is around Rs 2,200 for the fingerprint device and around Rs 8000-9000 per integrated biometric system / unit. Hence, the service organizations may issue a simple paper identification card to the beneficiary with his domain ID and minimum personal details instead of the Smart Card.

Further, in case of Aadhaar System of authentication, the bank details need not be obtained by the service organisations from the beneficiaries and the same need not be captured on the smart card. Once the records pertaining to the beneficiary and his nominees may be seeded with Aadhaar in service domain database and their respective bank accounts are also seeded with Aadhaar, any payment can be easily made to the beneficiary or its nominee over the Aadhaar Payment Bridge (APB). The system of APB is successfully being utilized by many organizations. Further, the beneficiary or its nominee can change their respective bank accounts at any time and seed Aadhaar in the new bank accounts avoiding the need to update the details of new bank accounts in the smart Card database.

For issue of smart card, the organisations operating programmes /schemes collect biometric information of individuals listed in their data-base. Since UIDAI has built up a robust biometric system, the collection of biometrics by the individual organization amounts to duplication of work. Instead, the organisation may undertake measures to seed their database with Aadhaar number of individuals, and utilize authentication services provided by UIDAI for verification of such individuals.

It may also be noted that while the identity of an Aadhaar holder can be established by any one of the 10 fingerprints and 2 Iris by online authentication, the offline authentication based on fingerprints biometrics stored on the Smart Cards would be restrictive and incapable of handling the cases of biometric exceptions.

## 4. Aadhaar Authentication Offerings

Authentication is the process of matching a person's identity details against the stored database, based on the credentials offered. Authentication User Agencies (AUAs) or their Sub AUAs can use the Aadhaar authentication services on its own or in conjunction with their own existing authentication system. Various AUAs/ Sub AUAs shall have different requirements for the degree of assurance required for authenticating beneficiaries/ customers based on the convenience to residents/ customers, number of beneficiaries, underlying purpose, criticality and stringency levels, penalties and costs associated with inaccurate authentication and technological feasibility. Various aspects that that provide strength in authentication are authentication factors, authentication attributes and authentication environment.

Authentication Factors

One factor or multiple factors could be used for authentication, such as:

1. What you have: Something the user uniquely has (e.g., a card, security token or cell phone/ OTP)

2. What you know: Something the user individually knows as a secret (e.g., a password, secret question or domain specific Personal Identification Number (PIN))

3. Who you are: Something the user individually is or does (e.g., fingerprint, iris pattern, signature).

Authentication Attributes

Demographic attributes like name, date of birth, address etc., OTP/ Cell phone and biometric attributes like fingerprint and/or IRIS shall be used for Aadhaar Authentication either as a single factor or in combination (multi-factor).

Authentication Environment

The authentication environment and trust worthiness may be classified as below:

| Environment / Mode | AUA Operator Assisted | Self-Service |
|---|---|---|
| AUA Managed and Monitored | Highly Trusted (Environment is fully managed by AUA and monitored by people, camera, etc. and application is operated by trusted operators, employees, etc. Examples include airline check-in counter etc.) | Semi Trusted (Environment is managed and monitored by people, camera, etc., but, the service itself is selfservice where resident conducts transaction by him/herself, Examples include Bank ATM, etc.) |
| Not managed and monitored | Semi-trusted (These are operated by employees or trusted operators, but, environment is not necessarily managed or monitored by people, cameras, etc. Examples include Bank BC Counter, HR Application, etc.) | Un-trusted (These are neither operated by trusted people nor managed or monitored with people/cameras, etc. Examples include self-service bill payment kiosks, self-service office entry point, Internet/mobile apps, etc.) |

AUA should make a comprehensive risk assessment as well as consider the environment factors before making a decision on the number of factors, additional

security and audit measures and the authentication offering to choose. In cases where the authentication is done in a highly trusted environment for services with lower risk assessment, the AUA may choose lower number of factors for authentication. In cases where the authentication is done in un-trusted environments for services with relatively higher risk, the AUA may put in place stronger security infrastructure and more factors for authentication.

## 4.1 Aadhaar Authentication Offerings

UIDAI shall provide demographic, biometric and OTP authentication services to AUAs. UIDAI advocates the federated authentication system wherein, AUAs are encouraged to use Aadhaar Authentication in conjunction with AUA's existing authentication system. AUAs or their Sub AUAs can use Aadhaar authentication services on its own or in conjunction with their own authentication system.

The AUA shall assess the convenience and interests of the resident and the risks/ impact/ consequence of inaccurate authentication and decide on the authentication offering required. In cases where the AUA perceives high probability of spoofing instances, the AUA may consider using multi-factor authentication to eliminate occurrence of such instances.

UIDAI offers the following Aadhaar Authentication offerings:

1. Type 1 Authentication
2. Type 2 Authentication
3. Type 3 Authentication
4. Type 4 Authentication
5. Type 5 Authentication

While Type 1 Authentication is based on demographic attributes, Types 2, 3, 4 and 5 provide additional factors such as biometric and/or OTP. The Aadhaar number all by itself shall not be a factor for Authentication. In general, a biometric/ OTP based authentication offers a higher degree of authentication assurance than a demographic authentication system.

### 4.1.1 Type 1 Authentication

Type 1 Authentication is based on demographic attributes. The AUAs can use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, etc. as per the API specifications) of a resident in the CIDR with the data in the AUA's database, on

a periodic basis to check validity of the credentials or for cleaning up the AUAs database by removing duplicates.

AUAs can also use demographic authentication for authenticating beneficiaries/ customers/ subscribers prior to any transactions.

NOTE: Type 2 to Type 5 described below provide additional “factors” to strengthen the authentication and may have demographics data as part of it.

### 4.1.2 Type 2 Authentication

UIDAI offers Type 2 Authentication offering, where the AUA shall authenticate residents based on One-Time-Password (OTP)/ Mobile. This offering (single factor authentication) may be used for authenticating residents where deployment of biometric technology is difficult or not practical.

### 4.1.3 Type 3 Authentication

UIDAI offers Type 3Authentication offering, where the AUA shall authenticate residents based on either one of the biometric modality (single factor authentication) using Fingerprint or Iris.

### 4.1.4 Type 4 Authentication

UIDAI offers Type 4 Authentication offering, where the AUA shall authenticate residents based on either one of the biometric modality (Fingerprint or Iris) and OTP/ Mobile. A combination of fingerprint/ Iris and OTP (two factor authentication) shall give a higher degree of authentication assurance.

### 4.1.5 Type 5 Authentication

UIDAI offers Type 5 Authentication offering, where the AUA shall authenticate residents based on Fingerprint, Iris and OTP. A combination of fingerprint, Iris and OTP/ Mobile (three factor authentication) shall give a higher degree of authentication assurance.

## 4.2 Attributes for each Aadhaar Authentication Offering

The table below provides the attributes for each Authentication Offering. The AUA can choose any attribute/ combination of attributes to achieve the assurance level.

| Authentication Offering | Aadhaar Authentication Attributes |
|---|---|
| Type 1 | Authentication Attributes:<br>Any single/ combination of the following attributes can be used<br>1. Name<br>2. Address<br>3. Date of Birth and other demographic attributes, as per the API document |
| Type 2 | 1. One-time-password (OTP)/ Mobile<br>Any of the demographic attributes also may be used |
| Type 3 | Authentication Attributes:<br>1. Either of Fingerprint or Iris Biometrics<br>Any of the demographic attributes also may be used |
| Type 4 | Authentication Attributes:<br>1. Either of Fingerprint or Iris and<br>2. OTP/ Mobile<br>Any of the demographic attributes also may be used |
| Type 5 | Authentication Attributes:<br>1. Fingerprint and<br>2. IRIS and<br>3. OTP/ Mobile<br>Any of the demographic attributes also may be used |

The AUA shall assess the business requirement and may opt to choose biometrics as an attribute for authentication only when the requirement is proportionate and appropriate for the use of biometrics. The AUAs are encouraged to follow the federated authentication model and use Aadhaar Authentication in conjunction with domain specific identifiers and identity credentials as extra authentication attributes to strengthen the AUA's authentication process.

## 5. Biometric Exception Handling

In any identity authentication program it is important to decide what exception rate is acceptable and how to handle the biometric exception cases. There is no particular biometric modality that can be used to authenticate everyone without exception. So like any other technology even biometrics has exceptions. There will always be a set of population who will be temporarily or permanently excluded from a specific biometric system. We can term this set of people as 'outliers'. Therefore Aadhaar

authentication system includes an effective approach where it can accommodate these outliers without causing inconvenience, discrimination to the residents and at the same time not compromising on security aspect. The outliers may fall into one of the following categories:

- People with missing biometric characteristic, for example: No iris or no fingers
- People with hard manual labor (like construction, mine workers) having all of their fingers in extremely poor condition with respect to fingerprint quality
- Injured people having cut finger, broken hand.
- People having illness such as cataract problem, burnt 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

Biometric exception can be classified under two categories (i) Failure to acquire (FTA), (ii) Failure to use (FTU).

Failure to acquire (FTA) means the failure of a biometric system to capture an image of sufficient quality and extract biometric data. FTA cases will be mostly associated with the temporary outliers. Firstly, it is very critical to understand the reason for FTA. If the environmental set up is the main reason, for example, in case of Iris, if stray illumination sources or bright lighting conditions is causing iris camera not to acquire an iris, then these condition should be eliminated and a resident should be asked to re-submit his/her Iris. In case of fingers, if FTA is due to extremely dry or dirty skin condition, then a resident may be asked to wash his fingers and then reinsert the finger. Sometimes additional advice/instruction or help from an operator can help in generating a reasonable quality biometric (example: for blind people bringing iris handle held close to the eye and guiding resident to align the iris, for people with arthritis, guiding/helping resident to place finger flat on the sensor or selecting an alternate finger).

In some cases alternate biometric modality can also be used, for example use iris if finger fails or vice versa or alternate biometric samples. For example, (i) use middle finger and thumb instead of just index finger for authentication (ii) use right iris instead of left iris.

It is recommended that in FTA cases, a resident should be allowed to provide multiple attempts (say 3 or 4) with a proper assistance before concluding that a biometric cannot be acquired.

Failure to use (FTU) means the conditions where biometric attributes (fingerprint and/or iris) does not exist or all biometrics are of extremely poor quality. FTU cases are associated with the permanent outliers. Manual intervention/ override have to be implemented for Failure to Use (FTU) cases. Intervention should be done by authorized personnel or operator in any of the following modes:

- Demographic verification: The resident's demographic detail can be obtained from CIDR and verified with the demographic details submitted at the Point of Service/ Authentication point.
- OTP based authentication: In case of FTA/ FTU cases, the operator can use OTP for authentication of the resident.
- Document verification and Photo Verification: By verifying valid Proof of Identity/ Proof of Address documents/ valid Photo identity cards, the operator can establish the authenticity of the resident with reasonable accuracy.

In order to avoid security issues, inconvenience to resident and streamline the process for exception cases (FTU and FTA), it is strongly recommended that the authentication application should have an option to record these cases along with AUA/operator details for better analytics and problem resolution. For the FTA cases, number of manual override attempts should be tracked and only limited number of manual overrides should be allowed per day per terminal to prevent operator malpractice.

## 6. Smart Card based Authentication

To overcome the issues involved in manual verification of the beneficiary at the point of service delivery, the organisations have been issuing Smart Cards to the beneficiaries for validation of the beneficiary at the Point of Sale (PoS) terminal. The personal details, photo, biometrics etc in the card are locally verified with the beneficiary at the service delivery point. The Smart Card has so far been quite useful for the purpose as the databases have been localized and the system does not require online connectivity.

Now with advancements in technology, the service providers have centralized their databases, internet facility is being increasingly available across India on real-time basis and UIDAI has achieved high level of Aadhaar saturation, the Smart Card system needs to be replaced by Aadhaar Authentication service.

As detailed in Para 3, Aadhaar Authentication service offers distinct advantages over Smart Card offline authentication system in terms of being nationally portable, highly scalable, easy to integrate with the client application, cost effective, and easy to

update & maintain. Organisations may avoid use of Smart Cards and design their systems to use one or more type of Aadhaar Authentication offered by UIDAI for validation of beneficiary at service delivery point.