सत्यमेव जयते

Aadhaar

Authentication Implementation Model

Operating Model

Version 1.0

AADHAAR

Unique Identification Authority of India
(UIDAI)

Table of Contents

Abbreviations and Terms

UIDAI	Unique Identification Authority of India
CIDR	Central Identities Data Repository is a logical collection of one or many UIDAI data centers where the central technology infrastructure required to issue Aadhaar numbers, update resident information, and authenticate the identity of residents is available.
False Reject	The instance of a system failing to detect a match between the input pattern and a matching template in the database
FRR	False Reject Rate – the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
False Accept	The instance of a system incorrectly matching the input pattern to a non-matching template in the database
FAR	False Accept Rate – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.
PID	Personal Identity Data
PII	Personal Identity Information (or Personally Identifiable Information)
ICDS	Integrated Child Development Services
JSY	Janani Suraksha Yojana
KYC	Know Your Customer
KYR	Know Your Resident
MSP	Managed Services Provider is an entity proposed to be appointed for management of CIDR
NREGA	National Rural Employment Guarantee Act
PDS	Public Distribution System
RSBY	Rashtriya Swasthya Bima Yojana
SLA	Service Level Agreement
SSA	Sarva Shiksha Abhiyaan

1 Introduction to Aadhaar Authentication Service

1.1 Service Definition

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

Prima facie, authentication qualifies as a service to be performed by UIDAI, as and when the National Identification Authority is setup under the Act of parliament. UIDAI shall offer Aadhaar-based authentication as a service that can be availed by government / public and private entities/agencies that wish to authenticate the identity of their customers / employees / other associates (based on the match of personal identity information) before providing them access to their services / business functions / premises, etc.

Some key features of Aadhaar authentication service are:

a) UIDAI shall offer Aadhaar-based authentication services free of charge till December 2013.

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

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

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

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

1.2 Service Description

1.2.1 Introduction to the Service

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

UIDAI, in its "Aadhaar Authentication Framework" document has listed the various authentication types that it offers. For each service that they wish to enable by Aadhaar authentication, user agencies choose an authentication type depending on their business requirements. The PID collected by the user entity for authentication is determined by the authentication type chosen.

This document addresses itself to the operating model for online[1] authentication of an Aadhaar holder's identity, i.e., where an Aadhaar holder's PID that is fed into the authentication device at the time of authentication are compared with the corresponding PID stored in UIDAI's Central Identity Data Repository (CIDR).

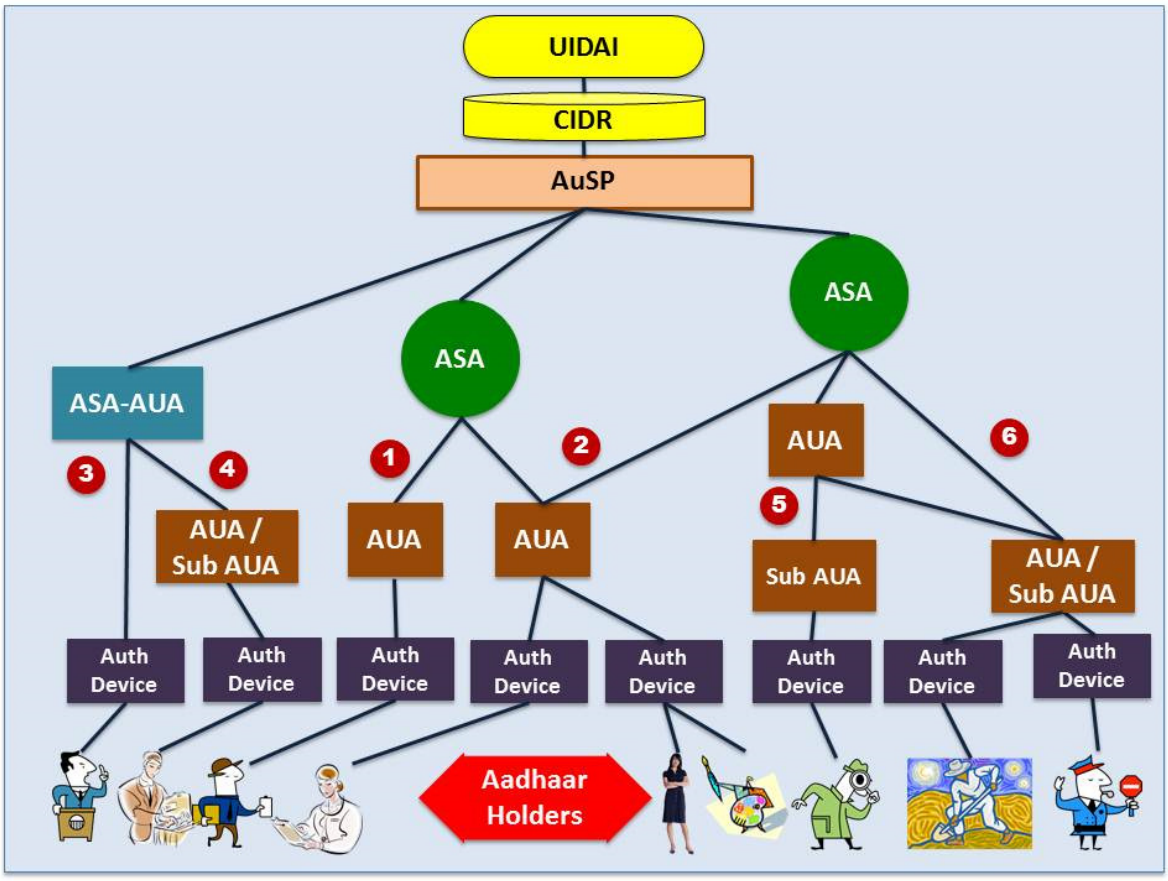
When an Aadhaar-holder claims their identity to seek access to a government or business service, proof of their identity is sought. The specific PID sought by the service provider is based on the authentication type of their choice. The collected PID is transmitted to CIDR which matches the received PID with the data existing at CIDR against the given Aadhaar number and determines whether the authentication is an "*accept*" or a "*reject*". The result is communicated to the authentication device where the authentication request has originated. No Personal Identity Information (PII) is returned as part of the response.

1.2.2 Introduction to Key Actors in Aadhaar authentication

The following figure identifies the key actors in the Aadhaar authentication model and depicts six possible scenarios in which the key actors could engage with each other. Brief description of key actors and the scenarios in which they engage with each other follow the figure. Detailed descriptions of key actors, their roles, responsibilities and

[1] Offline authentication is where the identity information collected at the time of authentication by the authentication device is compared to those stored elsewhere such as on a smartcard that is carried by the identity holder.

obligations of each actor and how they engage with each other in the Aadhaar authentication ecosystem follow in subsequent sections of this document.



1. **Unique Identification Authority of India (UIDAI):** UIDAI is the overall regulator and overseer of the Aadhaar authentication system. It also owns and manages, either by itself or through an agency, the Central Identities Data Repository (CIDR) that contains the personal identity information / data of all Aadhaar-holders. Presently UIDAI will manage the CIDR through a Managed Service Provider (MSP).

2. **Authentication Service Provider (AuSP):** AuSP is the entity that offers Aadhaar-based authentication services on behalf of UIDAI. To start with, the role of AuSP will be played by the entity that is the MSP. In the future, as authentication volumes go up, it is possible that more AuSPs are added to the authentication ecosystem.

3. **Authentication Service Agency (ASA):** ASAs are agencies that have established secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (see below for description of AUA) and transmit AUAs' authentication requests to CIDR. Only agencies contracted with UIDAI as ASAs shall send authentication requests to the CIDR; no other entity can directly communicate

with CIDR. An ASA could serve several AUAs; and may also offer value added services such as multi-party authentication, authorization and MIS reports to AUAs. Such value added services (over and beyond the basic Aadhaar authentication service) are not covered in this operating model. An ASA is bound to UIDAI through a formal contract.

4. **Authentication User Agency (AUA):** AUAs are agencies that uses Aadhaar authentication to enable its services and connects to the CIDR by itself (as an ASA) or through an existing third party ASA. It is also possible that an AUA engages more than one ASA. In order to directly connect to the CIDR, an AUA needs UIDAI's approval to become an ASA. An AUA could also transmit authentication requests from other entities that are "Sub AUAs" under it (see details on Sub AUA below). AUAs can also act as an aggregator offering authentication services to Sub-AUAs below them and may also offer value added services such as multi-party authentication, MIS reports and authorization to their Sub AUAs. An AUA enters into a formal contract with UIDAI in order to access Aadhaar authentication.

5. **Sub AUA:** An agency / entity (any legal entity registered in India) desiring to use Aadhaar authentication to enable its services could become an AUA or it could access Aadhaar authentication services through an existing AUA. In the latter case, it becomes a Sub AUA of the existing AUA which it engages. The following are some possible examples: (i) Government of any State/Union Territory could become an AUA and several ministries/departments in the State could access Aadhaar authentication services through the State government as its Sub AUAs. (ii) A small entity or business (e.g. a small scale bank) which does not want to directly engage in a formal contract with UIDAI but still wants to use Aadhaar Authentication, may choose to access Aadhaar services as a Sub AUA of an existing AUA (e.g. a large bank or any aggregator AUA offering AUA services). (iii) Several entities could combine under a single AUA for business reasons. Ex. Several hotels could access Aadhaar authentication as Sub AUAs of an Hoteliers Association that becomes an AUA. In all such cases UIDAI has no direct contractual relationship with the Sub AUA. Only the AUA is contracted to UIDAI and shall be responsible for all authentication requests flowing through it, including those originating from its Sub AUAs.

6. **Authentication Devices:** These are electronic actors that form a critical link in the Aadhaar authentication service. These are the devices that collect personal identity data (PID) from Aadhaar holders, prepare the information for transmission, transmit the authentication packets for authentication and receive the authentication results. They could be operator-assisted devices or self-operated devices. Examples of authentication devices include desktop PCs, laptops, kiosks,

handheld mobile devices, etc. They could be operated by the AUA (or the Sub AUA) or agents of AUA / Sub AUA.

7. **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 or their Sub-AUAs.

The above figure also depicts six possible scenarios in which key actors in the Aadhaar authentication ecosystem could engage with each other (numbered 1-5 in the figure):

1. **Scenario-1:** In this scenario, entities that become an AUA choose to connect to the CIDR through any of the existing ASAs. Examples: (i) A government department (say Department of Civil Supplies) becomes an AUA and chooses to connect to the CIDR through an existing ASA, possibly a telecom carrier that has already established secure leased line connectivity to the CIDR. (ii) A bank becomes an AUA and chooses to connect to the CIDR through an existing ASA, possibly an organization such as National Payments Corporation of India (NPCI).

2. **Scenario-2:** This scenario refers to the case where an AUA chooses to engage multiple ASAs to connect to the CIDR. Possible reasons why AUAs may choose to do so include business continuity planning (to ensure continuous availability of Aadhaar authentications service even if one ASAs services fail) and accessing different value added services from different ASAs.

3. **Scenario-3:** An entity such as a large bank becomes an AUA and chooses to directly connect to the CIDR by establishing secure leased line connectivity to CIDR. In this case it is an AUA and is also its own ASA. Such entities can also offer ASA services to other AUAs (this case is described as Scenario-2).

4. **Scenario-4:** This is an extension of the earlier scenario. In this case, the ASA-AUA (such as a large bank) that establishes its own secure leased line connectivity to the CIDR serves other AUAs / Sub AUAs (such as other smaller banks that choose to engage an ASA rather than establish their own leased line connectivity to the CIDR). The latter entity could connect to the ASA-AUA as an AUA (in which case it is directly contracted to UIDAI) or as a Sub AUA of the ASA-AUA.

5. **Scenario-5:** Some entities desiring to use Aadhaar authentication may choose to route their requests through an existing AUA rather than becomes AUAs themselves. In such cases, they become Sub AUAs of existing AUAs. Possible examples have been provided earlier in this section.

6. **Scenario-6:** Some AUAs may choose to transmit some of their Aadhaar authentication requests through an ASA and the remaining through another AUA.

This could happen when the latter AUA provides value added services that the former AUA desires to access (such as providing reconciliation services to banks in funds transfer transactions). A possible example: a bank could go through its ASA for services such as balance inquiry and go through a large bank for services such as funds transfer. In such cases, the bank plays the role of an AUA when going through an ASA and at the same time is a Sub AUA of another AUA (the larger bank) when going through the larger bank.

More details regarding key actors, their roles, responsibilities and obligations and how they engage with other actors in Aadhaar authentication ecosystem are addressed in Sections 2 and 3.

1.2.3 Federated mode of Aadhaar authentication service

UIDAI offers Aadhaar authentication that can be used alone or in conjunction with AUAs/Sub-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 could 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). Such revocable, local authentication systems come with a set of strengths and limitations. Aadhaar authentication system, on the other hand, could be described as "global" (because of its applicability across situations, AUAs and services) and "non-revocable" (because Aadhaar identity factors such as fingerprints and iris scans cannot usually be revoked/replaced). Global, non-revocable/permanent authentication systems come with their own set of strengths and limitations.

In the federated authentication model, the global-irrevocable Aadhaar authentication co-exists with and strengthens the local-revocable authentication of AUAs. It is expected that 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.

Aadhaar authentication should not be considered as a replacement for existing authentication systems, rather a complimentary scheme. UIDAI encourages complimentary authentication frameworks that may be specific to a domain/application, to take advantage of Aadhaar as a global identity system. For example, an online identity provider (as an AUA) may use Aadhaar and provide User ID

and password based authentication for Internet applications. In that case, that AUA uses Aadhaar authentication while creating initial User ID and password and then allows residents to use that User ID and password for logging into various Internet applications. When there are no local authentication schemes, AUAs/Sub-AUAs may use Aadhaar authentication 'as-is' and still gain great value in strongly identifying their customers/ beneficiaries.

The following are some types of situations where an AUA or a Sub-AUA could use Aadhaar authentication:

1. **One time usage:** When enrolling a new customer or creating a new service account for an individual. Examples are the issuance of a new PAN card, a new passport, creation of a new bank account or an internet service account for an online business. The AUAs in all such cases could authenticate an applicant's identity using the applicant's Aadhaar PID before issuing their own authentication factors.
2. **Periodic usage:** AUAs can also use Aadhaar based authentication system for periodic update of their customers' (or employees' or associates') identity information. Examples are using Aadhaar authentication as a basis for renewing an Aadhaar holder's KYC data, the address of a bank account holder, etc.
3. **Regular transactional usage:** AUAs/Sub AUAs can also use Aadhaar authentication system for carrying out any of their business transactions. Examples include banks that authenticate a customer's Aadhaar PID as well as bank-related identity information (account number/user id along with password/OTP, etc.) before enabling banking transactions such as funds transfer, funds withdrawal, etc.

Aadhaar authentication must therefore be viewed as a way to strengthen AUAs'/ Sub AUAs' existing authentication systems, rather than as a replacement for AUAs' existing authentication systems. 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 own local authentication to render the overall authentication system stronger and more reliable.

2 Engagement Model: Roles, Responsibilities and Obligations of Key Actors

The following key actors in the Aadhaar authentication ecosystem will be studied in detail in this section. For each of the key actors, this section identifies their role, how they enter the Aadhaar authentication ecosystem, and their key responsibilities and obligations.

1. UIDAI
2. Authentication Service Provider (AuSP)
3. Authentication Service Agency (ASA)
4. Authentication User Agency (AUA)
    a. Sub AUA
    b. Authentication Device (AD)
5. Aadhaar holder

2.1 Unique Identification Authority of India (UIDAI)

2.1.1 Role of UIDAI

Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to eligible applicants, and also defining the usages and applicability of Aadhaar for the delivery of various services. UIDAI offers online authentication of Aadhaar holders' identity, a service that can be used by government / public / private agencies to enable their services / business functions that require establishing of the identity of their customers / employers / associates.

UIDAI is also the overall overseer and regulator of the Aadhaar-based authentication ecosystem.

2.1.2 Responsibilities and Obligations of UIDAI

i. UIDAI issues Aadhaar number to eligible applicants.

ii. UIDAI is the custodian of all issued Aadhaar numbers and their corresponding Aadhaar-based Personal Identity Data / Information (PID/PII).

iii. UIDAI provides update services and other related lifecycle services to residents for managing their PID within CIDR.

iv. UIDAI provides Aadhaar-based authentication services to AUAs that wish to use Aadhaar Authentication for establishing identity of Aadhaar holders before providing access to their services.

v. UIDAI determines the operating and engagement model for Aadhaar-based authentication.

vi. UIDAI shall determine the rules regarding the usage of Aadhaar number and Aadhaar authentication.

vii. UIDAI determines the eligibility criteria for ASA, facilitates the application and registration of ASAs and enters into contracts with ASAs.

viii. UIDAI determines the eligibility criteria and entry process for AUA, facilitates the application and registration of AUAs and enters into contracts with AUAs.

ix. UIDAI determines standards and specifications that will be adhered to by all those participating in the Aadhaar authentication ecosystem (including ASA, AUA and Sub AUA). The standards and specifications include systems and processes, API specifications, infrastructure specifications (including device specifications), process specifications, technology specifications, certification specifications (if any), audit specifications, security specifications and SLAs (service level agreements) where applicable. In summary, UIDAI shall determine minimum standards and specifications for Aadhaar authentication and ecosystem partners may extend and add further specifications and standards to meet their domain and application needs. Please refer to documents published on UIDAI's website for the standards and specifications prescribed by UIDAI. UIDAI may choose to certify all applications that will be used by AUAs (and Sub AUAs) in enabling their Aadhaar authentication operations. This would include:

   - Certification (by itself or through approved independent certification agencies) of applications (such as applications driving the authentication systems and applications in the AUAs' systems) that will be used by AUAs and other participants in their Aadhaar authentication systems.

   - Certifying fingerprint and iris sensor and extractor pairs that will be incorporated in authentication devices. It is the responsibility of vendors of sensor and extractor pairs to get their products certified by Standardisation Testing and Quality Certification (STQC) Directorate and for using the same in their devices

x. UIDAI reserves the right to conduct audits of all key actors in the authentication ecosystem including ASA and AUA – either by itself or through UIDAI-appointed/approved independent audit agencies to examine compliance to its standards and specifications. As part of these audits, UIDAI/audit agency could

inspect the premises, operations and systems, infrastructure, security, etc. of the audited entity.

xi. UIDAI retains the right to take appropriate action against parties not complying with UIDAI's specifications including disqualification to use Aadhaar authentication system / termination of contract with UIDAI after appropriate grace period for remedial action as provided in the respective contracts.

xii. UIDAI shall provide a framework for the Dispute Resolution Mechanism for the Aadhaar authentication ecosystem.

xiii. In the future if any charges are associated with Aadhaar authentication, UIDAI could determine the charges or determine the framework to determine charges.

xiv. UIDAI will play any role when necessary to ensure that the system continues to offer uninterrupted services and run successfully.

2.2 Authentication Service Provider (AuSP)

2.2.1 Role of AuSP

a) Authentication Service Provider (AuSP) is responsible for the provisioning of Aadhaar authentication services on UIDAI's behalf.

b) AuSP's main areas of responsibility include authentication transaction operations (i.e., receive authentication request, execute a match of PID received with the identity information on CIDR and transmit the result), network operations, data centre operations, availability of authentication service, SLAs with AUA if any and monitoring operations & performance metrics.

2.2.2 How AuSP enters the Aadhaar Authentication ecosystem

a) To start with, when the authentication volumes are expected to be low, the role of AuSP will be played by the Managed Service Provider (MSP). In future, as authentication volumes increase, it is envisaged that more entities will play the role of AuSP.

b) At that time, UIDAI will determine the process of adding more AuSPs to the Aadhaar authentication ecosystem; and manage the process to bring in more AuSPs.

2.3 Authentication Service Agency (ASA)

2.3.1 Role of ASA

a) ASA is an agency that has established secure leased line connectivity to the CIDR to transmit authentication request on behalf of AUAs and receive response back from CIDR. ASAs build and maintain their secure connectivity to CIDR in compliance with the standards and specifications set by UIDAI. Examples of ASAs are:

   i. A government department such as a State's IT Department could become an ASA and establish a secure UIDAI-compliant leased line connectivity to CIDR through which several ministries/departments in the State could channel their authentication requests.

   ii. A telecom carrier that obtains UIDAI's approval could establish a secure leased line connection with the CIDR and offer ASA services to AUAs.

   iii. An organization such as National Payments Corporation of India (NPCI) could establish a secure UIDAI-compliant leased line connectivity to CIDR and offer authentication services and possibly value added services to banks.

b) ASAs receive Aadhaar authentication request from AUAs and transmit the same to CIDR. In turn they receive CIDR's response that they transmit back to the AUA that has placed the authentication request.

c) An ASA could serve more than one AUA.

d) It is conceivable that some ASAs offer value added services to AUAs in addition to providing them with connectivity to CIDR. Examples of value added services include authorization services, MIS and funds reconciliation (in case of banking). However, such arrangements over and beyond basic Aadhaar authentication service that an ASA and an AUA may enter into are not the concern of UIDAI and are out of the scope of this document.

2.3.2 How ASAs enter Aadhaar Authentication ecosystem

a) The eligibility criteria for an agency to be considered for engagement as an ASA are as under:

A. The agency should either be

i. A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government

OR

ii. An Authority constituted under the Central / State Act

OR

iii. A Not-for-profit company / Special Purpose organization of national importance

OR

iv. 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:

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

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

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

B. 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.

b) ASAs enter Aadhaar authentication ecosystem through UIDAI's ASA appointment process determined and conducted by UIDAI.

c) Entities wishing to act as ASA apply to UIDAI providing necessary information along with supporting documents where relevant. UIDAI shall examine the applications and approve qualifying applicants as ASA. Approved ASAs enter into a contract with UIDAI and are permitted to build secure leased line connections to the CIDR that comply with UIDAI's standards and specifications.

d) It is envisaged that UIDAI's ASA appointment process is open and continuous, i.e., applicants could file in their applications any time and could be appointed if they qualify. However, UIDAI could change this policy at a later point.

e) Each ASA contract is for a specified duration at the end of which an ASA is free to apply for a renewal. UIDAI shall evaluate the renewal application and approve renewals for qualifying applications.

2.3.3 Responsibilities and Obligations of ASA

i. ASAs shall adhere to their contract with UIDAI in complying with UIDAI's standards and specifications including SLAs if relevant.

ii. The ASA shall ensure that all their infrastructure and operations including systems, processes, IT and biometric infrastructure, security, etc., are compliant with UIDAI's standards and specifications.

iii. When an ASA receives an authentication request from an AUA, it is recommended that the ASA performs basic checks on the authentication input before forwarding it to CIDR. The authentication request is forwarded to CIDR only if it is compliant and complete. Else, it is returned to the AUA with appropriate error message (who then forwards it to the authentication device with necessary instructions).

iv. On receiving the response from CIDR, ASA transmits the result of the transaction to AUA that has placed the request.

v. It is highly recommended that the ASA maintains logs of all authentication transactions it processes. These logs shall be retained for specified duration determined by UIDAI and shall be shared with other entities only on need-basis. These logs shall capture transaction details such as Aadhaar number, requesting AUA, timestamp, etc. but not PID associated with an authentication transaction. The storage of transaction logs shall comply with the applicable laws of the country like the IT Act 2000 etc.

vi. In conducting their operations, the ASA shall comply with all applicable laws and regulations in the country in the areas of data security and management like IT Act 2000.

vii. The ASAs shall ensure that its systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body before commencement of its operations and the ASA shall provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, etc. issued by UIDAI, in this regard, from time to time.

viii. The ASAs shall ensure that its operations and systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body on an annual basis and the ASA shall provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, etc. issued by UIDAI, in this regard, from time to time.

In addition to this, UIDAI reserves the right to audit ASAs by itself or through agencies appointed / approved by UIDAI. During these audits, the ASA shall cooperate fully with UIDAI / audit agency and provide access to their premises, procedures, records, systems, personnel and any other relevant part of their authentication operations. In case of non-compliance, UIDAI could take appropriate action (such as termination of contract after appropriate grace period for remedial action). The cost of the audits is borne by the ASA.

ix. The ASA shall keep UIDAI informed of the list of AUAs it serves. On entering into a contract with a new AUA, the ASA informs UIDAI (along with the details sought by UIDAI) before commencing service to the new AUA. Similarly when an ASA disengages with an AUA, the ASA shall inform UIDAI within 7 days of the disengagement.

x. The ASA may have a contract with the AU A and may provide any value added services to the AUA as part of that contract. However, such value added services do not form part of Aadhaar Authentication.

xi. The ASA shall be responsible to UIDAI for all their authentication related operations (as covered in the contract between UIDAI and the ASA). Even if the ASA outsources parts of its operations to other entities, the responsibility for the operations and results of authentication related operations lies with the ASA.

xii. In case of investigations around authentication related fraud or dispute, the ASA shall extent full cooperation to UIDAI (or their agency) and/or any other authorized investigation agency. This includes providing access to their premises, records, systems, personnel, infrastructure, any other relevant resource / information and any other relevant aspect of its authentication operations.

2.4 Authentication User Agency (AUA)

a) AUA is any agency that seeks to use Aadhaar authentication to enable its services. Each AUA can use Aadhaar authentication to enable one or more of its services. The AUA chooses an appropriate authentication type for each of the services enabled by Aadhaar authentication. An AUA has the option of connecting to the CIDR by itself or through an existing ASA.

b) Examples of AUA:

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

   b. A bank that seeks to authenticate its customers before letting them complete a financial transaction such as withdrawal or transfer of funds. Such transactions could be operator-assisted (when they take place in the bank's premises) or self-operated (as in internet banking).

   c. The administration/security department of a high-security building/zone that seeks to authenticate individuals seeking entry into the building/zone.

   d. A social networking site/ e-commerce website that seeks to authenticate customers/ subscribers during the registration process

2.4.1 Role of AUA

a) The AUA is the principal entity that drives authentication requests to enable their services. An AUA can use Aadhaar authentication to enable one or more of their services. Based on the result of the authentication, the AUA determines whether or not to provide Aadhaar-holders access to their services.

b) An AUA could send its authentication requests directly to CIDR (in which case it needs UIDAI's approval to become an ASA) or engage an existing ASA for transmitting its authentication requests. An AUA could also engage more than one ASA if they wish to.

c) The AUA shall ensure that the authentication request originating at an authentication device is compliant with the standards and specifications prescribed by UIDAI (refer Appendix I) and complete before transmitting the request to its ASA. After the AUA receives the result of the authentication from CIDR, it determines whether or not to provide service to the Aadhaar-holder; and it transmits the authentication result to the originating authentication device along with instructions on the next steps.

d) It is also possible for AUAs to transmit authentication requests originating from Sub AUAs under it. Sub AUAs are entities that wish to use Aadhaar authentication to enable their services, but choose to connect to the CIDR through an existing AUA rather become AUAs themselves. Details about Sub AUAs can be found in Section 2.5.

2.4.2 How an AUA enters the Aadhaar Authentication ecosystem

a) The agency should either be:

i. A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government

OR

ii. An Authority constituted under the Central / State Act

OR

iii. A Not-for-profit company / Special Purpose organization of national importance

OR

iv. A bank / financial institution / telecom company

OR

v. A legal entity registered in India that seeks to use Aadhaar authentication to enable its services. Applications from such agencies would be considered and approved by AUA Approval Board to be constituted by UIDAI.

The agency should give an undertaking and demonstrate the capability to implement and maintain the infrastructure and systems required to become an AUA.

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

b) Agencies seeking to use Aadhaar-based authentication to enable their services shall apply to UIDAI by providing necessary information along with the required supporting documentation as well as the information on the ASA through which the AUA shall connect to the CIDR.

c) On receipt of necessary information (and documentation if relevant), UIDAI approves an AUA. On approval, the AUA and UIDAI enter into a contract. As long as the role of AuSP is played by the MSP, AUA need not enter into a contract with the AuSP. However, if more players start playing the role of AuSP, AUAs might

have to enter into contracts with one/more AuSP (on issues such as authentication SLAs) before they can start availing Aadhaar authentication services.

2.4.3 Responsibilities and Obligations of AUA

i. For each service for which they would like to use Aadhaar authentication, the AUA chooses an appropriate authentication type and shall inform UIDAI regarding the same. The choice of authentication type in turn, indicates the specific identity information to be sought from the Aadhaar-holder to enable that service. Details of authentication types offered by UIDAI can be found in the "Aadhaar Authentication Framework" document. The choice of authentication type for a service is a decision of the AUA alone; and none of the other entities including UIDAI and ASA are responsible for this decision. It is possible for an AUA to change the authentication type of any service if it so desires, under intimation to UIDAI.

ii. The AUA shall adhere to the processes and the AUA on-boarding checklist provided by UIDAI for getting started with Aadhaar authentication service. As and when there are any changes in the parameters, the AUA shall keep UIDAI informed of the list of its services that are enabled by Aadhaar authentication. This process is expected to be done, possibly in a self-service mode (such as an online update through UIDAI portal).

iii. The AUA shall establish its authentication related operations (including systems, processes, technology, infrastructure, security, etc.) in compliance with UIDAI's standards and specifications.

iv. AUA shall be responsible for provisioning of network from authentication devices to the AUA server and between the AUA server and the ASA server, and shall ensure compliance to UIDAI's security specifications. In addition, they shall be responsible for procuring and deploying any hardware/software/certificate/etc. for complying with Aadhaar authentication standards.

v. AUA shall ensure that devices used for Aadhaar authentication are procured, deployed, and managed by them or their agent(s) in compliance with UIDAI specifications and standards published by UIDAI from time to time.

vi. The AUA shall log all its authentication transactions and maintain them for a specified period of time. The logs shall capture details of an authentication transaction but not corresponding PID. The storage of transaction logs shall

comply with applicable laws and regulations of the country like the IT Act 2000 etc. The details of logs stored, the duration of storage and any other aspect of data storage shall be determined by UIDAI specifications, regulations applicable to the AUA's service and industry, the AUA's own requirements and other applicable laws and regulations.

vii. It is highly recommended that the AUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analysing authentication related transactions to identify fraud cases and patterns. If the AUA is a victim of a fraud or identifies a fraud pattern through its fraud analytics system, it shall share all necessary details of the fraud with UIDAI.

viii. The encrypted PID block should not be stored, unless it is for buffered authentication for a short period of time, and after transmission, it should be deleted. Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database. The AUA shall ensure that all relevant laws and regulations are adhered to in relation to data storage and data protection (with regard to Aadhaar-based identity data) in their systems, that of their agents (if applicable) and with authentication devices.

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

x. The AUA shall ensure that its systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body before commencement of its operations and the AUA shall provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, etc. issued by UIDAI, in this regard, from time to time.

xi. The AUA shall ensure that its operations and systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the audit report should be shared with UIDAI upon request. It is the AUA's responsibility to ensure that their Sub AUAs and agents are also regularly audited.

In addition, UIDAI reserves the right to audit the AUA's operations and systems (and their agents if applicable), by itself or through an auditor appointed by UIDAI. During these audits, the AUA shall cooperate fully with the audit agency and provide them necessary access to their premises, procedures, records,

systems, personnel and any other relevant aspect of authentication operations. In case of non-compliance, UIDAI could take appropriate action (such as termination of AUA contract after suitable grace period for remedial action). The cost of these audits shall be borne by the AUA.

xii. The AUA is responsible for identifying exception-handling mechanisms and back-up identity authentication mechanisms when Aadhaar-based federated authentication fails. Authentication failures could occur due to process failures, infrastructure failures (including power, IT infrastructure, authentication devices, network connectivity) or biometric failures (where Aadhaar holder's biometric cannot be acquired or used for some reason).

xiii. When an AUA associates with a Sub AUA (details of Sub AUA in Section 2.5), the AUA shall inform UIDAI of the engagement before starting to serve the new Sub AUA. Similarly, when a Sub AUA disengages with the AUA, the AUA shall inform UIDAI within 7 days (or a period specified by UIDAI) of disengagement. The process of such updates is envisaged to be in a self-service mode (such as an online update through UIDAI portal). When an AUA engages with a Sub AUA, it generates a Sub AUA Code to identify the specific Sub AUA. When informing UIDAI of its engagement with the Sub AUA, the AUA also informs UIDAI of the new Sub AUA Code. When transmitting authentication requests from a Sub AUA, the AUA always includes the Sub AUA Code so that Aadhaar authentication transaction logs can track the origin of all authentication requests. It is necessary that for each Sub-AUA, a separate license key is used so that the engagement and disengagement of Sub-AUAs can be easily accomplished by creating and revoking their respective license keys.

xiv. It is the AUA's responsibility to ensure that all Sub AUAs under it are regularly audited for compliance with UIDAI specifications. In case of non-compliance or default, the AUA shall report the same to UIDAI and take correction action according to UIDAI's guidelines.

xv. When an AUA engages a Sub AUA, from UIDAI's perspective, the AUA is responsible for the connectivity between the Sub AUA's authentication devices to the AUA's systems.

xvi. Even if the AUA outsources parts of its operations to 3rd party entities, the responsibility for the authentication operations and results lies with the AUA. The AUA is also responsible for ensuring that the authentication related operations of such 3rd party entities comply with UIDAI standards and

specifications and that they are regularly audited by approved independent audit agencies.

xvii. In case of investigations around authentication related fraud or dispute, the AUA shall extend full cooperation to UIDAI (or their agency) and/or any other authorized investigation agency. This includes providing access to their (and if applicable their agents') premises, records, personnel, systems, relevant resource / information and any other relevant aspect of authentication operations.

xviii. An AUA shall proactively inform UIDAI of any misuse of Aadhaar data, authentication services, or any compromise of Aadhaar related data or systems within their network.

2.5 Sub AUA

a) Sub AUAs are agencies that access Aadhaar authentication through an existing AUA.

b) An entity desiring to use Aadhaar authentication could choose to become an AUA or it could choose to access Aadhaar authentication services through an existing AUA. In the latter case, it becomes a sub AUA of the existing AUA which it engages.

c) Possible examples:

   a. Nodal department such as the IT Department/ e-Governance Department of any State/Union Territory could become an AUA and several ministries/departments in the State could access Aadhaar authentication services through the Nodal department as Sub AUAs.

   b. Several entities, conceivably in similar business, could combine under a single AUA for business reasons. Ex. Several hotels could access Aadhaar authentication as Sub AUAs of a Hoteliers' Association that becomes an AUA

   c. Entities that have infrequent Aadhaar authentication requirements may choose to access Aadhaar services as Sub AUAs of existing AUAs.

2.5.1 Role of Sub AUA

a) A Sub AUA is similar to an AUA in its usage of Aadhaar authentication. The primary difference is that an AUA is contracted directly to UIDAI whereas a Sub AUA enters into a contract with the AUA it engages.

b) A Sub AUA can use Aadhaar authentication to enable one or more of their services. Based on the result of the authentication, the Sub AUA determines whether or not to provide Aadhaar-holders access to their services.

2.5.2 How a Sub AUA enters the Aadhaar authentication ecosystem

a) An entity desiring to become a Sub AUA identifies the AUA to engage with and applies to the AUA by providing necessary information and supporting documentation if necessary.

b) The Sub AUA commits to compliance with UIDAI standards and specifications in their Aadhaar authentication operations.

c) The AUA informs UIDAI of the engagement with the Sub AUA and commences its services to the Sub AUA.

2.5.3 Responsibilities and Obligations of Sub AUAs

The responsibilities of a Sub AUA will be similar to that of an AUA. The responsibilities and obligations of an AUA covered in Section 2.4.3 will be applicable to Sub AUA as well.

2.6 Authentication Devices

Authentication devices are electronic actors in the Aadhaar authentication system where an Aadhaar authentication transaction is initiated. These could be operator-assisted or self-operated devices. Examples of authentication devices include desktop PCs, laptops, kiosks and handheld mobile devices that are, if required, integrated with / connected to biometric devices (for capturing fingerprints and/or iris scans).

2.6.1 Role of Authentication Devices

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

a) Collect PID from Aadhaar holders.

b) Perform basic checks on the information collected for completeness and compliance.

c) Prepare the authentication data packet for transmission.

d) Transmit the authentication packets for authentication.

e) Receive the authentication results along with instructions for next steps if any.

2.6.2 How Authentication Devices are deployed in the Aadhaar authentication ecosystem

a) Authentication devices could be deployed in the Aadhaar authentication ecosystem by the AUA, Sub AUA or the agents of AUA/Sub AUA.

b) AUAs/ Sub AUAs shall be responsible for provision of network from devices to AUA/ Sub AUA server and to AUA/ ASA server and ensuring security. In addition, they shall be responsible for procuring and deploying any hardware/software/certificate/etc. for complying with Aadhaar authentication standards.

2.6.3 Features of Authentication Devices

i. They are compliant with UIDAI standards and specifications

ii. Authentication devices could be operator-assisted or self-operated.

iii. They must be capable of collecting relevant information from Aadhaar holders, prepare authentication data packets (PID block), performs structural validation of data, transmit data packets and receive authentication results along with instructions on next steps if any. Collection of Aadhaar information by the authentication devices shall be carried out in compliance with UIDAI specifications.

iv. Authentication devices must be deployed such that they cannot retain Aadhaar holders' biometric and OTP data captured for the purposes of Aadhaar authentication during an transaction (except in case of *Buffered Authentication* described in Section 3.1, in which case they will be able to store encrypted data for a certain period of time).

v. In terms of data storage, authentication devices must comply with all applicable laws and regulations of the country like IT Act 2000, etc.

2.7 Aadhaar Holder

A holder of Aadhaar-based identity (Aadhaar-holder) is any eligible individual who has enrolled with UIDAI and obtained their unique Aadhaar number. In the context of Aadhaar authentication, they are usually associated with AUAs (or Sub AUAs) as customers, employees or associates; and in this capacity, seek access to AUAs' / Sub AUAs' services.

2.7.1 Role of Aadhaar-Holder

a) Aadhaar-holders are the owners of their PID stored in the CIDR. They are generally associated with AUA / Sub-AUA as customers/ beneficiaries/employees/ associates, etc. and seek access to the AUA's / Sub AUA's services. In order for them to gain access to these services, their identity is authenticated using their Aadhaar-based identity information (and AUA / Sub AUA-based identity information where relevant).

b) Depending on the authentication type sought by AUA/Sub AUA, they provide their Aadhaar-related demographic and/or biometric identity information before they are provided access to the service they are seeking.

c) They enjoy rights and privileges and are subject to obligations as identified in the "Aadhaar Holders' Charter" of Aadhaar-based authentication service.

d) *Examples:*

a. An individual who goes to a fair price shop to get her monthly ration of rice.

b. A bank account holder who goes to a bank where she holds an account to conduct a financial transaction such as withdrawal or transfer of funds; or a bank account holder who wishes to complete a financial transaction through internet banking from her home computer.

c. An individual who has to produce proof of identity while applying for a new telephone connection.

2.7.2 How Aadhaar-holders enter the Aadhaar Authentication ecosystem

a) Eligible individuals seeking Aadhaar identity enter the Aadhaar ecosystem when they enrol with one of the UIDAI-approved registrars by providing their demographic and biometric identity information.

b) Upon successful completion of the enrolment process, each eligible individual obtains his or her unique Aadhaar number. The demographic and biometric identity information of each Aadhaar-holder is stored against the corresponding Aadhaar number in the CIDR.

2.7.3 Responsibilities and Obligations of Aadhaar-Holder

i. Aadhaar-holders shall provide their consent to provide and to be authenticated using their Aadhaar-based PID sought by the AUA / Sub AUA and shall provide the Aadhaar based PID voluntarily in order to gain access to the AUA's / Sub AUA's services they wish to access.

ii. It is the Aadhaar-holders' responsibility to keep their PID in the CIDR valid and current. They do so on a periodic-basis or on a need-basis as the case may be. Some instances where an update may be necessary:

a. Informing UIDAI of a change in address

b. Updating the collection of fingerprints on a periodic basis

c. Correction of any errors

iii. Aadhaar holders shall approach UIDAI in case they have reason to believe that their Aadhaar PID has been compromised by any of the actors in the authentication ecosystem.

iv. Aadhaar holders shall proactively inform UIDAI of any misuse of Aadhaar data or authentication services.

v. Their rights, responsibilities are obligations are covered in detail in the Aadhaar Holders' Charter.

3 Variation of the Engagement Model: Buffered Authentication

There may be cases where the authentication model described above undergoes minor variations. One such case is Buffered Authentication.

a) In some situations, it is envisaged that the AUA will not be seeking real-time authentication from CIDR. Possible examples include:

    a. When connectivity is not available or possible at the point of PID collection preventing real-time transmission of authentication requests.

    b. When the nature of AUA's service does not require real time authentication or is not suitable for real time authentication (as when a very high number of authentications have to be completed within a short duration and the AUA's service can do without real time authentication. Ex. attendance tracking scenario).

b) In such cases, PID of multiple Aadhaar-holders are collected and buffered at the authentication device; and transmitted at a later time. This is referred to as *Buffered Authentication*.

c) The Buffered Authentication process therefore varies slightly from that of the normal case till the authentication requests are transmitted from the authentication device. From this point, the model and process is similar to the normal scenario – the buffered set of authentication requests are checked by the AUA and transmitted to ASA, who further performs structural validation of data and forwards to the AuSP; upon receiving the authentication result for each request, the ASA forwards them to the AUA who forwards the same to the authentication device that has placed the requests.

d) Even though the authentication device may transmit multiple authentication requests at the same time, each authentication request will be treated as a separate transaction in the Aadhaar authentication system and each authentication request will have its own *Auth code*.

e) It is the AUA's responsibility to ensure that the authentication devices being used are capable of managing Buffered Authentication (which may include capability to store multiple authentication requests, transmit them at the same time, and receive and store results of multiple authentications; and necessary security features).

f) There will be an upper limit for the duration of time that authentication requests can be buffered. This duration will be determined by UIDAI specifications.

g) Since Buffered Authentication is provided only for supporting occasional connectivity issues on the field, buffering of authentication requests should be done *only* on authentication devices and not on the servers of Sub AUA / AUA / ASA.