UIDAI STRATEGY OVERVIEW

CREATING A UNIQUE IDENTITY NUMBER

FOR EVERY RESIDENT IN INDIA

UNIQUE IDENTIFICATION
AUTHORITY OF INDIA

Table of Content

1.0 Executive Summary

In India, inability to prove identity is the biggest barrier that prevents the economically weaker & the marginalized sections of society from accessing benefits, subsidies and commercial services from service provider agencies in both public and private sectors across the country because they require proof of identity and address before provisioning a service or benefit for individuals, however, till date there remains no nationally accepted, verifiable and portable identity number which addresses the issue stated above.

As a result, every time individuals seeking benefits or services, undergo a full cycle of identity verification. Different service providers have different requirement and process of verification of identity which leads to inconvenience to individuals, prolongs verification process and turns out to be expensive for service providers. This gives rise to the need of an identity proof which is universally accepted and verifiable to ensure effectiveness of KYC (Know your Customer) at minimal cost to the service provider

In a bid to issue a universally accepted identity card to all residents, the Government of India through Election Commission undertook an effort in 1993 to issue photo identity cards. Subsequently, in 2003, the Government of India approved issue of Multipurpose National Identity Card (MNIC) which led to launch of "Aadhaar" program through establishment of *Unique Identification Authority of India* (UIDAI) in January 2009 as an attached office to the erstwhile Planning Commission (now NITI Aayog). The objective of UIDAI is to issue a unique identification number (Aadhaar) to all Indian residents which is robust enough to eliminate duplicate and fake identities and can be verified & authenticated in an easy, cost-effective way.

Through Aadhaar program, Government of India clearly envisaged the following benefits:

a. Fool-proof and Robust identification of residents
b. Lower transaction costs.
c. Transformation of delivery of social welfare programs by making them more inclusive of communities, now marginalized, from such benefits due to lack of identity.
d. Allow the government bodies to shift from indirect to direct benefits transfer through electronic channels.

2.0 Objectives of Aadhaar Program and Strategy

In pursuance to fourth meeting of Empowered Group of Ministers (EGoM) dated 04.11.2008, UIDAI was constituted and notified vide notification# No. A.03011/02/2009-Adm.1 dated 28.01.2009 as an attached office under erstwhile Planning Commission (now NITI Aayog). The EGoM outlined the strategy of Aadhaar program and recommended, inter alia, the following responsibilities of UIDAI.

2.1 Key Roles and Responsibilities

SL. No.	Roles and Responsibilities of UIDAI
1.	Lay down plan and policies to implement UID Scheme, own and operated UID database and own responsibility of its updation and maintenance on an on-going basis
2.	Implementation of UID scheme to entail, inter alia, following key responsibilities i. Generate and Assign UID to residents ii. Define mechanisms and processes for interlinking UID with partner databases on a continuous basis iii. Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis_ iv. Define usage and applicability of UID for delivery of various service v. Take necessary steps to ensure collation of NPR with UID (as per approved strategy) vi. Evolve strategy for awareness and communication of UID and its usage vii. Frame policies and administrative procedures related to hiring / retention / mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all State units under UIDAI

2.2 Features of Aadhaar

Subsequent to notification of UIDAI, several committees were constituted to outline the objective and character of Aadhaar which will have the potential to evolve as a common identity tool across all domains in both public and private sector. In the table below, salient features of Aadhaar have been explained:

SL. No.	Feature	Description
1.	Only a 12 digit number	Given the huge population of India and considering the growth in future a 12-digit number will be adequate for generating approximately 80 billion unique ids
2.	Random Number without any intelligence	Aadhaar number is a randomly generated number which does not provide any PII [1]about the Aadhaar holder.
3.	Minimal data	In order to remain domain agnostic, Aadhaar captures minimal resident attributes which can be uniformly applied to all services for unique identification of beneficiaries/ customers viz. Name, Date of Birth/ Age, Gender, Address, Photograph and biometrics (fingerprint & Iris)
4.	Numbers once issued shall never be reissued	Aadhaar number is issued by UIDAI only once to a resident. The number remains valid for the entire life of the resident

[1] PII – "Personal Identifiable Information" such as Name, Address, Gender etc. which may be used to construct one's identity

SL. No.	Feature	Description
		and even after death. The number is never issued to another resident
5.	Aadhaar is for all residents	Aadhaar is issued to all residents even new born children
6.	Uniqueness ensured through biometrics	Biometrics of a resident, fingerprint and Iris, captured during enrolment process are unique to every resident. The same is used to establish uniqueness of the resident in the database
7.	Aadhaar does not confer Citizenship, Rights & Entitlements	Aadhar is an identity tool ONLY therefore does not confer citizenship, rights and entitlements.
8.	Security & Privacy of Resident data	Aadhaar by design ensures security and privacy of residents' data collected through enrolment process. Access to authentication services are given only to authorized ecosystem partners of UIDAI. Under no scenario, biometric data of residents is shared
9.	Ubiquitous Online Authentication Platform	UIDAI provisions an authentication platform accessible only to authorized ecosystem partners from all parts of the country at all times to authenticate Aadhaar holders using their Aadhaar number and demographic/OTP/ biometric attributes.

2.3 Biometrics Design Standards& Multi-ABIS Strategy

One of the features of Aadhaar, as stated above, includes establishing uniqueness of one's identity through biometrics which essentially requires development & adoption of certain biometrics standards in order to achieve this objective uniformly across people, processes and systems. UIDAI, upon notification, constituted a biometrics standards committee with the mandate a) to develop biometric standards that will ensure interoperability of devices, systems & processes used by various agencies that use the UID system and b) to review the existing standards of biometrics and, if required, modify/ extend/ enhance them to serve the specific requirement of UIDAI related to de-duplication & authentication.

As per the mandate, the committee deliberated on the three biometrics that may be potentially used. As a first step, committee studied the relevant reports published in western countries, where biometrics based application have been in use for a very long time. However the committee was aware of the challenges in the Indian context vis-à-vis effectiveness of the technology for a billion+ population and varying quality of biometrics.

The committee compared the effectiveness of each type of biometric attributes for reliable de-duplication and authentication. In the table below, comparative study may be referred.

Biometric Attribute	Comments
Face	Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources however it is not considered a robust biometric for effective de-duplication & authentication because face may be disguised leading to false negative response (falsely rejecting one's identity).
Fingerprint	This is the most commonly used biometric attribute across the world but the large variation of quality of fingerprint in India may pose challenge to implementation of a reliable solution. Fingerprints can be captured using very low cost devices which facilitates its adoption.
Iris	Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore, the iris would be a good biometric for pure de-duplication applications. However large scale adoption of Iris requires high degree of user cooperation owing to use of contact lenses or small Iris and upfront investment into expensive devices.

The Biometric Standards committee, in its final report, recommended capturing of all three biometrics viz. face, fingerprint & Iris at the time of enrolment. It recommended use of only fingerprint and Iris for authentication. In order to ensure interoperability of biometrics data across various devices and system, committee recommended use of following ISO/IEC standards:

Biometric Data Type	ISO/IEC Standard	Enrolment	Authentication
Finger Minutiae Data	ISO/IEC 19794-2:2005	Yes	Yes
Finger Image data	ISO/IEC 19794-4:2005	Yes	Yes
Face Image data	ISO/IEC 19794-5:2005	Yes	No
Iris Image data	ISO/IEC 19794-6:2005	Yes	Yes

For more information, please refer Biometrics Standards Committee report on UIDAI's website[2]

The Aadhaar system is designed to service the entire population of India, and will involve the biometric identification of at least 1.2 billion residents. Since the estimated database size is larger than any of the previous known biometric databases, the biometric sub-system needs to be constantly monitored for accuracy, scalability and performance. Since de-duplication at this scale has not been previously attempted anywhere in the world, it was decided to procure three (3) ABIS (*Automatic Biometric Identification System*) vendors to perform biometric de-duplication as a risk mitigation strategy.

[2] Biometric Standards Committee Report:
http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

Multi-ABIS approach will ensure that a) there is no vendor lock-in b) the three ABIS service providers compete for accuracy and throughput c) there is a higher accuracy of de-duplication by aggregating result from all the three ABIS in the event of detection of a duplicate and d) there exists ability to de-duplicate even poor quality biometrics data

2.4 Demographic Data Standards

UIDAI constituted DDSVP (Demographic Data Standards and Verification Procedure) committee to standardize commonly used demographic data to identify residents and also establish their verification procedure. Larger objective of this exercise was to aid interoperability across various systems and business processes that capture and work with residents' identity.

Since, the primary object of Aadhaar was inclusion, the committee recommended capturing minimal data which can apply uniformly across both public and private sectors domain to effectively identify residents. Based on the recommendation of the committee following data fields were recommended with standardized attributes.

2.4.1 Enrolment Data

Information	Fields	Mandatory	Data Type
Personal Details	Name	Yes	Varchar (99)
	Date of Birth	Yes	Date
	Gender	Yes	Char(1) – M/F/T
Address Details	Residential Address	Yes	8 address lines and PIN code
Parent's/ Guardian's Details	Father's/ Husband's/ Guardian's Name	No	Varchar(99)
	Father's/ Husband's/ Guardian's UID	No	Number(12)
	Mother's/ Wife's/ Guardian's Name	No	Varchar(99)
	Mother's/ Wife's/ Guardian's UID	No	Number(12)
Introducer Details	Introducer's Name	Conditional	Varchar(99)
	Introducer's UID	Conditional	Number(12)
Contact Details	Mobile Number	No	Varchar(18)
	Email Id	No	Varchar(254)

2.4.2 Verification Procedure

In order to build a trusted database of residents, it is essential that demographic data is verified before issuing Aadhaar number. The three distinct methods of verification are a) Based on supporting document b) Based on Introducer system c) Based on NPR (National Population Register) process of public scrutiny d) Based on Head of the family as introducer. The DDSVP committee recommended the following broad principles of verification viz. Ease of Access, No Harassment, No Discrimination, No Corruption and No Exclusion.

Demographic Field	Process of Verification
Name	Name is verified against any one of the proofs of identity listed. A copy of

	Proof of Identity should be kept as part of enrollment and verification should be done against the original document. In the case of resident not having a valid Proof of Identity document, resident should furnish the form signed by any of the approved introducers.
Date of Birth	Date of Birth is verified against the proof of date of birth submitted. In case of lack of a valid document, approximate date of birth (Declared or Approximate) may be taken and marked so in enrolment record
Address	The addresses are verified against any one of the valid proof of address submitted at the time of enrolment.

Refer DDSVP committee report on UIDAI's website[3]

2.5 Benefits to the Residents (Aadhaar Holders)

Through Aadhaar program, Government of India envisages following benefits for Aadhaar holders and service providers in both public and private sectors:

For Aadhaar Holders	
1.	One identity proof accepted across the country for welfare schemes and commercial services
2.	No requirement of submission of identity document every time a service is needed
3.	Online verifiable identity which can be verified in a fool-proof manner from any part of the country
4.	Targeted delivery of welfare & commercial services thus elimination of impersonation; ensured through biometric authentication
5.	Inclusion of economically weaker sections and other marginalized groups into service delivery framework
6.	No dependence on the "influential" people for obtaining access to services and benefits
For Government entities and commercial service providers	
7.	Biometric based fool-proof method of identification of beneficiaries and customers therefore n risk of impersonation
8.	Tool to de-duplicate beneficiaries' and customers' database to weed out duplicate entries and to identify ghost records leading to clean databases
9.	Reduced cost of KYC
10.	Enabler for direct transfer of monetary benefits into the bank accounts of beneficiaries

[3] DDSVP Committee Report http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf

2.6 Program Implementation Strategy

UIDAI envisions enrolling all the residents of India including the marginalized and economically weaker sections of the society and children. A program of the nature and size of Aadhaar requires creation and continuous enrichment of an ecosystem which effectively collaborates with members of the ecosystem to produce desired result. Key activities of the program include a) Enrolment & Data Update b) Authentication and c) Logistics consisting of letter delivery & Contact center operation. In order to implement these activities, UIDAI has defined discreet roles which the ecosystem partners adorn to deliver desired functionality of the ecosystem. Roles of all ecosystem partners is stated in the table below:

SL. No.	Ecosystem Partner	Responsibilities
1.	UIDAI	UIDAI is at the heart of this ecosystem, and is responsible for the definition and development of all relationships, policies and the core infrastructure. It is also responsible for measuring, and monitoring the performance of the system, and driving it towards delivering on its goals.
2.	Registrars	Registrars partner with UIDAI in enrolment of residents
3.	Enrolment Agencies	EAs are agencies which have been empanelled by UIDAI on their technical and financial capabilities. EAs enter into contract with registrars to enroll residents in the field with the help of their operators and supervisors, trained and certified by UIDAI
4.	Authentication User Agencies (AUA)/ e-KYC User Agencies (KUA)	AUAs & KUAs are service providers who leverage Aadhaar authentication service in their services for unique identification of their beneficiaries & customers
5.	Authentication Service Agencies (ASA)/ e-KYC Service Agencies (KSA)	ASAs & KSAs are entities that provide network connectivity services to AUAs and KUAs, respectively, to connect to UIDAI's CIDR (Central Identities Repository).

The timing of Aadhaar program roll-out coincides with growing social investment in India, a shift in focus to direct benefits, and with the spread of IT and mobile phones which has made the public receptive to technology-based solutions. An initiative of this magnitude also requires proactive participation of Central, State & local Governments, as well as public and private sector agencies across the country. With their support, the project seeks to realize a larger vision of inclusion and development for India.

Keeping the Aadhaar philosophy, as described in this section, UIDAI established processes for Enrolment of residents, Data Update & Authentication which have been elaborated in subsequent sections.

2.7 Project Risks

The UID project does face certain risks in its implementation, which have to be addressed through its architecture and the design of its incentives. Some of these risks include:

SL. No.	Project Risk	Mitigation
1.	Low Adoption	Aadhaar number is a randomly generated unique number, minimal data is captured during enrolment and the authentication platform of UIDAI is sufficiently generic in nature to remain relevant to almost all industry domains. Considering this attribute of Aadhaar, there is a huge potential to become a common identity tool across all industry domains. Additionally, riding on inclusion agenda of Aadhaar program, a large section of marginalized population of the country will now have an identity which will be accepted across the country
2.	Requirement of a very high scalability	Aadhaar platform has been designed for scale. It has the capability to handle 10 million transactions an hour which can be augmented further by low cost linear scaling of server farm
3.	No precedence of such large scale biometric based program	From technology perspective, a number of design choices have been made to ensure that the platform performs successfully under extreme conditions too involving large variation in biometric quality, very huge population, extreme weather conditions etc. Some of the design choices include: 1. Use of open source tools to maintain vendor neutrality 2. Multiple ABIS providers to ensure correctness of biometric matches 3. Deployment of landscape across multiple data centers for high availability and reliability 4. Robust data security 5. Low marginal cost
4.	Risk to privacy and security of residents' demographic and biometric data stored with UIDAI	UIDAI has deployed robust security infrastructure to prevent any unauthorized dissemination of demographic or biometric data of residents stored in CIDR. It may be noted that biometric data is never shared with any entity or individuals.

3.0 Aadhaar Enrolment & Data Update

Enrolment is the process by which residents voluntarily assert their identity and apply for an Aadhaar. The process of enrolment is a standardized and implemented uniformly across the country through an enrolment ecosystem consisting of Registrars & Enrolment Agencies and supported with technology by UIDAI. Entire enrolment process is monitored by UIDAI for data quality and consistency.

In the paragraphs below, enrolment strategy and the rationale have been explained in fair detail. It should be remembered that the objective of enrolment process has always been to enroll all the residents including those who have remained outside of social safety net on account of lack of identity & address proofs.

3.1 Types of Enrolment

Aadhaar is issued to all residents of the country including the new born children. Presently enrolment is being conducted through various channels like Permanent Enrolment Centers, Enrolment Camps and Mobile Enrolment Centers. At the enrolment center, the resident is provided with the necessary forms that must be filled, and a list of documents required for validating the identity information. Resident demographic and biometrics data are captured at the enrolment station using standard Enrolment Client software provided by UIDAI. Privacy of an individual is of utmost concern to the UIDAI therefore, for each and every enrolment, the standardized Enrolment Client requires the resident to provide his/her consent. The identity of the resident and proofs are verified by a registrar's official approved verifier at the enrolment center. The resident is issued an enrolment receipt. The resident data is then sent to the UIDAI for processing. On completion, the UIDAI issues a letter, which is delivered to the resident. Additionally, a copy of the Aadhaar letter can be downloaded from https://eaadhaar.uidai.gov.in .

3.2 Data Capture

During enrolment, a resident is expected to mandatorily submit one of the 18 approved identity proofs and 33 approved address proofs (*List of valid documents may be referred on UIDAI's website*[4]). Residents are also expected to submit a valid proof of date of birth if available and conditionally submit proof of relationship. Following attributes are captured during enrolment along with supporting documents:

Attribute	Mandatory/ Optional	Documentary Evidence
Name	Mandatory	Proof of Identity
Gender	Mandatory	Proof of Identity
Date of Birth	Mandatory*	Proof of Date of Birth
Address	Mandatory	Proof of Address
Biometrics (Fingerprint & Iris)	Mandatory	NA. Captured during enrolment
Photograph	Mandatory	NA. Captured during enrolment

[4] List of valid identity proofs and address proofs http://uidai.gov.in/images/commdoc/valid_documents_list.pdf

Email Id	Optional	NA. Captured during enrolment
Mobile Number	Optional	NA. Captured during enrolment
Relationship	Conditional	Proof of Relationship (Refer para 3.3.3)

* In India a large of number of residents do not possess a valid Date of Birth proof e.g. birth certificate, school leaving certificate, etc. which leads to necessary provisions in the enrolment process to enroll such people. UIDAI allows one of the following three types of date of birth during enrolment namely; Verified, Declared and Approximate. A *Verified* date of birth is one that is based on a documentary evidence submitted as valid proof of date of birth. *Declared* date of birth is one wherein the resident is aware of the date of the birth but does not have any supporting document as evidence. Lastly, *Approximate* date of births are those that not document based and are approximate & ascertained by trained enrolment operators.

During enrolment, resident data is captured in both English and one of the local language (*Assamese, Bengali, Gujarati, Hindi, Kannada, Konkani, Malayalam, Manipuri, Marathi, Nepali, Oriya, Punjabi, Tamil, Telugu and Urdu*) for higher level of adoption across the country.

3.3 Exception Management

Apart from the above mentioned normal method of enrolment, UIDAI prescribes methods through which residents who cannot undergo normal method of enrolment owing to lack of documents or biometrics can also be enrolled.

3.3.1 Missing Biometrics

UIDAI's enrolment process contains provisions to enroll residents for Aadhaar despite having incomplete biometrics attributes viz. missing or deformed fingers & iris. In such cases, all such exceptions are noted at the time of enrolment and the photograph is taken with complete view of missing biometrics, as evidence.

3.3.2 Introducer based Enrolment Process

A large section of residents in the country does not have a valid identity proof & address which can be submitted at the time of enrolment. Keeping inclusion as prime objective, UIDAI prescribes "Introducer" based system of enrolment whereby an Introducer, a person approved by Registrar, is entrusted to vouch for someone's identity in his/ her locality. In cases where residents are unable to present a valid identity & address proofs, Introducers confirm their identity and submit their own Aadhaar number during enrolment process for establishing traceability.

3.3.3 Head of Family based Enrolment Process

In large of households it is normally seen that only the head of family possesses valid identity & address proofs whereas others have none. In such cases, UIDAI has prescribed "Head of Family" based enrolment process wherein a head of family having a valid Aadhaar number vouches for the identity of his/ her family members. In this method of enrolment, Aadhaar number of the head of family is also

captured and a valid proof of relationship[5] with the head of family also needs to be submitted by the applicant.

3.4 Enrolment Client

Enrolment client is the standard software application, developed by UIDAI, which is used by all enrolment agencies across the country to enroll residents. The client is currently available for Windows and Linux based PCs. A special Android tablet based client called "Child Enrolment Lite Client (CELC)" has also been developed to enroll all children in the age group of 0 to 5 in an accelerated manner. The clients support the following functionalities:

Functionality	PC Client	CELC
Enrolment	Y	Y
Data Correction	Y	N
Data Update	Y	N
System Configuration	Y	Y
Client data sync	Y	Y
Enrolment Data Export	Y	Y

Both types of clients support capture of biometrics (Fingerprint, Iris), facial image and GPS coordinates. The clients are designed to ensure data security through strict access control, encryption and audit logs.

3.5 Enrolment Operator Ecosystem

Any biometric identity projectôs success primarily depends on the ó**Quality**ôof the data collected at the time of enrolment. In order to ensure superior quality of data being collected at the time of enrolment, UIDAI in partnership with training and certifying agency developed a ñTraining & Certificationò module.

The Enrolment Client has been designed in such a manner that unless an operator or supervisor responsible for operating the Enrolment Client is not Certified, he/she will be unable to login and undertake enrolment of any residents.

3.6 Demographic Data Validation

The enrolment client includes multiple validation rules for the enrolment data viz. data type, length of field & format which are reapplied on the server to ensure maximum compliance with the data validation rules. Verification procedure of each type of data is explained below:

3.6.1 Name and Address Validation

Demographic data verification is essentially performed in two steps. First level of verification is performed by designated supervisors at each enrolment center who verify the authenticity of documentary proofs submitted by residents before marking enrolment process complete. Second level of verification, apart from sanity checks performed by automated applications in UIDAI's CIDR, is performed by Quality Control operators at UIDAI who verify 100% of enrolment records for sanity. Such

[5] Valid proofs of relationships http://uidai.gov.in/images/commdoc/valid_documents_list.pdf

sanity checks are augmented by periodic audits of enrolment centers by the regional offices of UIDAI to ensure compliance with processes and submission of data with desired quality.

3.6.2 Master Data Sync

All the enrolment client stations are periodically synced with UIDAI's server in a secure manner to download latest PIN code mappings, list of permitted and blacklisted operators and other system configurations to ensure highest degree of compliance with latest directives issued by UIDAI from time to time.

3.7 Aadhaar Generation

At the end of enrolment process, residents are issued an enrolment slip which contains a unique 14-digit enrolment number and timestamp of enrolment. The two data elements refer to a unique enrolment record and can be used to fetch the record for future reference, say in case of status enquiry. Subsequent to enrolment, the data packet containing encrypted demographic & biometric data is uploaded to CIDR by the enrolment agency. Within CIDR, data packet is first assessed for sanity before being subjected to manual Quality Control. Enrolment records failing sanity checks are either rejected or put to further assessment however records meeting sanity check requirement are forwarded for Aadhaar generation.

At the time of Aadhaar generation, 1:N check is performed to check uniqueness of biometric record whereby biometric data in the enrolment packet is compared for another matching record in the entire database of Aadhaar holders. If an existing biometric record matches with that in the enrolment packet, then that enrolment record is construed as a case of duplicate enrolment because it is presumed that no two individuals can have same set of 10 fingerprints and 2 Iris.

If no match is found, then a 12-digit Aadhaar number is generated and the same is then communicated to the concerned resident through a printed Aadhaar letter or e-Aadhaar letter which is soft format of the printed Aadhaar letter. Subsequently, the biometric data of the resident is stored in an anonymized form to ensure further privacy and security of the data.

3.8 Aadhaar Data Correction

Subsequent to enrolment process, a resident may discover error in the demographic or address data submitted earlier. As per the process, a 96-hour window post enrolment is available to the resident to approach the enrolment agency to submit correction request.

3.9 Aadhaar Data Update

UIDAI allows residents to update their demographic data, address and biometric data and photograph whenever a change occurs or is found incorrect. Following updates may be carried out:

3.9.1 Demographic Data Update

UIDAI allows update of all data fields including address as and when changes occur or inaccuracies are found. While all fields can be updated more than once, date of birth can be updated only once. Nonetheless, sufficient safeguards have been built into the update process to prevent excessive updates.

In all cases of updates, residents are required to authenticate themselves either biometrically or through OTP (One Time Password) either at an enrolment station or through self-service Self Service Update Portal (SSUP) portal.

3.9.2 Photograph Update

Residents are allowed to update their photograph at enrolment stations subsequent to biometric authentication. At this time UIDAI has not defined mandatory photograph update policy but it is recommended that photograph may be updated after every 10-15 years.

3.9.3 Biometric Update

Biometric attributes captured during enrolment include 10 fingerprints and 2 Iris. UIDAI has provisioned for biometric updates. Below are the use cases of biometric updates:

a. Children below age of 5 are enrolled without their biometrics being captured as those attributes are not sufficiently developed at that age. However, at the age of 5, their biometrics are captured for the first time
b. Again, minors are expected to update their biometrics at the age of 15
c. All adult residents are allowed to update their biometrics whenever a need arises owing to age related changes or incorrect capture during enrolment

In all such cases of biometrics update, residents are expected to submit an update request at an enrolment station.

3.9.4 Update Channels

In order to extend convenience to residents, UIDAI has developed several channels for performing data updates:

SL. No.	Update Channel	Description
1.	Permanent Enrolment Centers	Permanent Enrolment Centers are managed by enrolment agencies empanelled by UIDAI. At these centers the EAs facilitate submission of update requests for all types of demographic and biometric data including photograph
2.	Self Service Update	All residents having registered mobile number may leverage the facility of online submission of update requests through UIDAI's website https://ssup.uidai.gov.in/ssup-home. Through the online method, a resident may submit update request for the following fields only: Name, Address, Date of Birth, Gender, Care Of& Email Address
3.	Requests by Post	A few limited fields are allowed to be corrected or updated by calling UIDAI Contact Centre and sending supporting documents via post. After manual inspection and approval, update packets are created by UIDAI and passed onto automated update flow. Following fields are allowed to be updated through this channel: Name, Address, Date of Birth, Gender, Care Of, Mobile Number & Email Address

In each of the above channels, residents are expected to mandatorily submit self-attested copies of relevant documentary proofs as supports.

4.0 Authentication & E-KYC Services

UIDAI offers an online authentication platform to authorized institutions to validate identity of Aadhaar holders. Presently two types of authentication services are offered by UIDAI namely *Authentication* and *E-KYC* which may be leveraged in the context of service delivery or other use cases. During the authentication process, the agency collects the Aadhaar number, along with other identity attributes (possibly including biometrics) and sends it to the CIDR for verification. The UIDAI responds with a Yes or No in the case of *Authentication* and entire demographic data including address & photograph in the case of *E-KYC*, thus authenticating the identity of the individual.

4.1 Philosophy

Effectiveness of an authentication services lie in answering the following three questions:

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

As explained in subsequent sections, Aadhaar authentication platform offers multiple modalities of authentication to answer the above questions for varying effectiveness.

4.2 Modalities of Authentication Services

Presently, UIDAI's authentication permits use of three modalities namely *demographic data*, *biometrics* & *OTP (One Time Password sent to registered mobile phone)* and combinations of the three for varying degrees of effectiveness. The diagram here depicts various modalities of authentication platform.

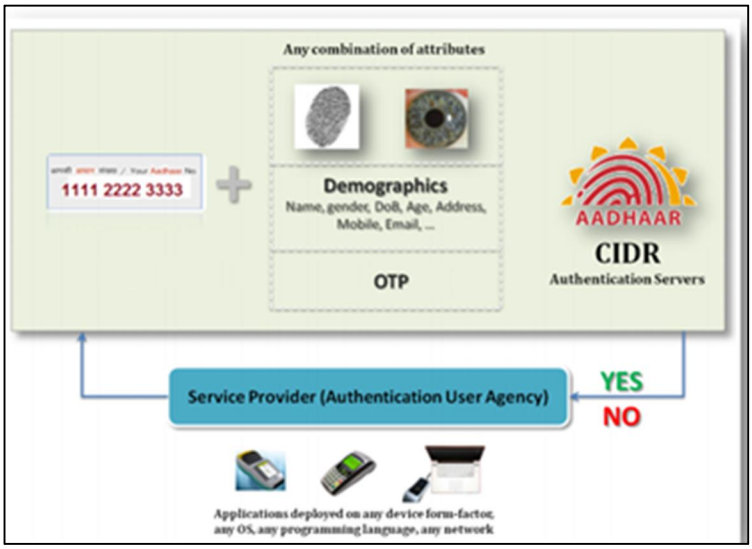

Figure 1: Aadhaar Authentication Modalities

Effectiveness of authentication can be ascertained with the number of modalities used in the process. As an example, an authentication performed with modalities viz. demographic data and biometrics will be more secure and

fraud-resistant than a transaction performed with only demographic data as the modality. Similarly, an authentication performed with all modalities used together will be more secure than a transaction with up to two modalities. Among, the modalities, it can be appreciated that all transactions requiring biometric modality are more secure than those not using it. This is primarily because biometric authentication requires presence of the Aadhaar holder and that it cannot be easily faked.

Types of modalities are explained below:

4.2.1 Demographic Authentication

In the case of demographic authentication, one or more demographic fields including address along with Aadhaar number are submitted to CIDR for authentication.

4.2.2 Biometric Authentication

Biometric authentication requires submission of one or more fingerprint and iris biometric attributes along with Aadhaar number to CIDR for authentication

4.2.3 OTP Authentication

Mobile number provided at the time of enrolment or during last data update becomes concerned Aadhaar holder's registered mobile number whereby the Aadhaar holder is presumed to be the owner of that mobile number. As part of OTP authentication, a one-time password is sent to the registered mobile of the resident undergoing authentication which is then fed back to complete the authentication process.

4.2.4 Combination of Modalities

Authentications may be carried with combinations of the above three types of authentications for better effectiveness.

4.3 Federated Authentication Model

Aadhaar being voluntary in nature, UIDAI recommends federated authentication models whereby Aadhaar authentication is used only to strengthen existing authentication systems of the user agencies. UIDAI also views existing authentication systems to be more specific to the industry domain in which they are used therefore Aadhaar authentication which is global & generic in nature should only be used to strengthen existing authentication systems. Nonetheless, it is the prerogative of the user agency to either use Aadhaar authentication in federated model or standalone.

4.4 Authentication Services

UIDAI offers two services through its online authentication platform namely a) Authentication and b) e-KYC. While "Authentication" service returns only a *Yes* or a *No* in response to an authentication attempt, e-KYC service returns entire demographic data including the address and photograph of the resident in case of successful match. However, it may be noted that no biometric data is returned under any circumstance. The schematic diagram below explains the two authentication services:

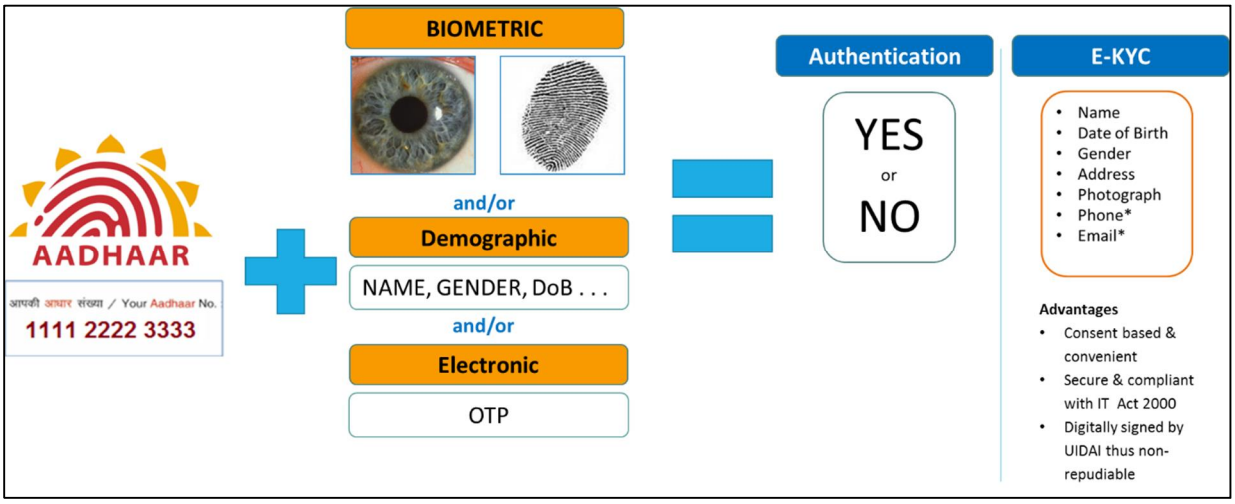

Figure 2: Aadhaar Authentication & e-KYC Services

4.5 Authentication Ecosystem

Authentication ecosystem consists of UIDAI and its partner organizations comprising

a) AUAs & KUAs are service providers or government entities who leverage Aadhaar authentication as part of their service delivery and

b) ASAs & KSAs who provide AUAs & KUAs secure network connectivity to UIDAI's CIDR.

AUA: Aadhaar User Agency
ASA: Aadhaar Service Agency
KUA: e-KYC User Agency
KSA: e-KYC Service Agency

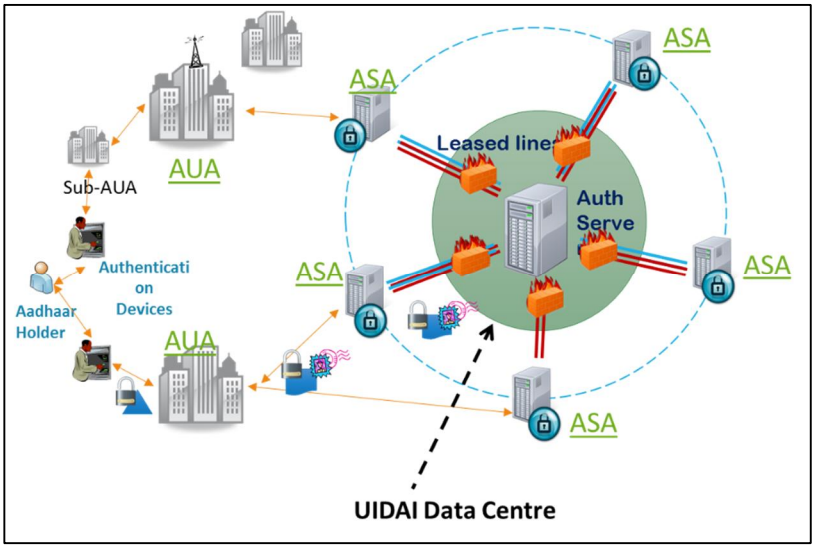

Figure 3: Aadhaar Authentication Ecosystem

UIDAI onboards each of the ecosystem partners through a detailed due-diligence and approval process in order to ensure that only qualified public & private sector entities are allowed access to authentication services and that there is a genuine need of the service. Terms of usage of platform are agreed through a Memorandum of Understanding which forms the basis of all the activities performed as part of the engagement. During the entire course of engagement, UIDAI holds the authority to discontinue access to any of the ecosystem partners if an evidence of inappropriate usage is detected or reported thus ensuring security of residents' data stored in CIDR.

4.6 Authentication Infrastructure

Keeping in view security of residents' data and high volume of transactions owing to huge population of the country, UIDAI has deployed a highly robust, secure and scalable authentication infrastructure. The infrastructure is designed to meet the following expectations:

- Multi data centers for high availability and reliability even in the event of an outage at one data center
- Sub-second response to avoid introduction of unnecessary delays in applications leveraging Aadhaar authentication
- Fully load balanced to address the need of scalability and speed
- Linear scalability architecture through simple expansion of server farm for achieving higher scalability
- Support for 100 million transactions per day.
- Maintenance of detailed audit trail for future references

4.7 Information Privacy & Security

Aadhaar authentication services are architected in such a way that without residents' awareness and explicit consent authentication cannot be carried out. This is to ensure that no AUA or KUA misuses resident data for undue benefits. As per the terms of usage agreed with UIDAI through Memorandum of Understanding, each AUA & KUA is mandated to capture a physical consent of Aadhaar holders in the service delivery application or on paper before conducting authentication.

Apart from the above safeguard, authentication APIs are protected by a robust security framework consisting of encryption, digital signature, access control and audits to protect any unauthorized access or usage of authentication services. All the aspects are explained below:

4.7.1 Personal Identifiable Information (PII)

PII refers to data which can be used to uniquely identify a single individual. From the data collected by the UIDAI the following is classified in this manner:

PII	Description
Aadhaar Number	Unique 12 digit number issued to residents
Demographic data	All demographic data including address except Gender, Age & Year of Birth and components of address unless they are not combined with other PII fields
Biometric data	All biometric records are considered PII
Enrolment Records	Resident data including the biometrics
Data Change Records	Resident data. May include biometrics too
Authentication Records	Aadhaar number and one or more PII data

While the demographic data that the UIDAI collects is already available with several agencies in the country – some of it is also available to the public (E.g., electoral rolls, railway reservation charts, telephone directories, etc.) - it is recognized as sensitive data within Aadhaar system, and handled with

due care. Similarly, the authentication records are designed to be sensitive to resident privacy concerns.

4.7.2 Access Control

Authentication services are accessible to the ecosystem partners only through APIs (Application Programming Interfaces) available over private leased lines which prevents direct access to any of the application servers or database servers. Additionally, access to the APIs is available only to white-listed IP addresses of ecosystem partners which prevents any unauthorized access.

It may also be noted that the access given to ecosystem partners is time bound which is ensured through use of randomly generated license keys. All communications of ecosystem partners with UIDAI requires sharing of license key which has a limited validity. At the end of validity of license keys, the keys are renewed subject to validity and good standing of terms stated in Memorandum of Understanding.

4.7.3 Encryption

All the communication between AUA/ KUA applications and CIDR remains in encrypted form unless the authorized entity, whether UIDAI or ASA/KUA, decrypts the information. As per the design of Authentication service, all PII including demographic information and biometric data are encrypted with a randomly generated session key using AES-256 symmetric algorithm (AES/ECB/PKCS7Padding) after which the key itself is encrypted using 2048 bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1Padding). Such a design ensures that the resident data while in transit remains encrypted and cannot be viewed by a hacker or any unauthorized entity watching the data traffic.

** Use of asymmetric key encryption method requires encryption of resident data with the public key of recipient by the sender and decryption by the recipient only using its private key.*

4.7.4 Digital Signature

Design of authentication service mandates use of digital signature to sign every data packet when exchanged between the ecosystem partners. Such an arrangement ensures integrity of data packets and non-repudiation. Presently, UIDAI allows use of Class II and III digital signatures for the purpose issued by Certifying Authorities authorized by Controller of Certifying Authorities, Govt. of India, under IT Act.

4.7.5 Audit Trails

All authentication transactions performed by AUAs & KUAs are logged in CIDR for future reference, say in case of inquiries or disputes. Nonetheless, logged information is agnostic of the business process or the context of authentication. Such a safeguard has been built into the system to prevent all possibilities of snooping and profiling of Aadhaar holders.

It may be deduced that the logged information is used only for resolution of technical issues which may be reported from the field either by ecosystem partners or Aadhaar holders.

4.7.6 Data Retention & Usage

Following table defines the period for which each type of data will be stored by UIDAI

Data Type	**Retention Period**
Aadhaar Number	Forever
Current Demographic data	Forever

Data Type	Retention Period
Current Biometric Data	Forever
Enrolment Record and archived data update records	Forever in archived form
Authentication Records	6 months in active audit and up to 7 years in archived storage
Transactions Aggregated records (no PII)	Forever
Master Data	Forever

UIDAI ensures through its strict security procedures that no PII data ever leaves the CIDR, except through an approved process, or with explicit resident consent.

4.8 Pricing

UIDAI may charge a nominal fee to the ecosystem partners to recover the marginal cost of usage of the platform however at the time of writing of this version of the document pricing structure hasn't been notified by UIDAI.

5.0 Aadhaar Enabled Service Delivery

From the advent of modern governance and structured commerce, both public and private service agencies across the country require their customers/ beneficiaries to establish their identity prior to provisioning of services to them. Traditionally, residents of India have used all types of identity proofs viz. Passport, Ration Card, Voter Id card etc. but never a true identity token to establish their true identity. Given the gap stated above, Aadhaar as an identity tool facilitates unique identification of Aadhaar holders with the help of their Aadhaar number and one or more demographic & biometric attributes or One-time password.

5.1 Challenges with existing identification procedures

In the absence of Aadhaar as an identity tool, all service providers in public and private sectors depend on documentary proofs e.g. copies of Passport, PAN card, Voter Id card, Ration Card so on and so forth which are often trusted but never verified. In a large number of cases it has been found that customers'/ beneficiaries' databases contain duplicate records, fake records which were inserted on account of weak verification procedures or lack of it. In effect, a number of frauds have come to light wherein services have been delivered to unintended beneficiaries who could either impersonate true beneficiaries or on account of duplicate records drew benefits more than the entitlement. Over a period of time, such vulnerable identification procedures have led to large amount of leakage of benefits causing unnecessary financial burden on the exchequer and not achieve the desired objective.

Efforts have been made by the service providers to strengthen identification procedures by incorporating physical verifications but those procedures have only escalated the cost of KYC (Know Your Customer) making the services more expensive and have caused long delays in their activation.

5.2 Application of Aadhaar

Technically, Aadhaar authentication can be used in any industry domain owing to the minimal data that is captured during enrolment and uniform application of biometrics or OTP for identification across all domains. Aadhaar is an IT enabled identity solution which needs to be leveraged appropriately by service agencies along with required business re-engineering and computerization of their services through eGovernance and ICT initiatives.

Until the end of November 2015, Aadhaar authentication has been leveraged in various services on pilot basis and on permanent basis too namely; Banking, Telecom, Scholarships, Subsidy Payouts etc. Moot point is that Aadhaar authentication has been uniformly used across industry domains without any modification which highlights its generic nature and establishes its effectiveness & applicability across domains.

5.3 Aadhaar Seeding as a Pre-requisite

All Aadhaar enabled applications require 100% digitization &seeding of customers'/ beneficiaries' databases with Aadhaar number. Aadhaar being a unique number can effectively weed out duplicate

records of same customer/ beneficiary and can also help out in weeding out records of fake customers/ beneficiaries. Aadhaar seeding procedures may be referred on UIDAI's website[6]

5.4 Aadhaar Usage Types

As stated earlier, Aadhaar authentication platform being generic in nature can be uniformly leveraged by all industry domains without any customization. Typical usages of Aadhaar relate to:

a. Unique Identification of Beneficiaries & Customers
b. Establishing proof of presence
c. As Financial Address

In the paras below, above usage types have been further elaborated:

5.4.1 Unique Identification

Aadhaar authentication process uses Aadhaar number and one or more demographic & biometric attributes or an OTP to uniquely identify a person. Since Aadhaar is issued after necessary biometric based de-duplication check in Aadhaar database it can be comfortably established that the person undergoing Aadhaar authentication is indeed the one who he/ she claims to be.

In order to leverage Aadhaar authentication, service delivery software applications should be appropriately modified to implement the same. UIDAI recommends use of federated authentication model whereby Aadhaar authentication is only used to strengthen the existing authentication procedure further however it is the prerogative of the service provider to use Aadhaar authentication as standalone or a federated one.

5.4.2 Establishing Proof of Presence

Aadhaar is an extremely effective tool in establishing proof of presence of the Aadhaar holder undergoing authentication. Submission of biometrics as part of authentication procedure is a sufficient evidence of the presence of the person.

5.4.3 Aadhaar as Financial Address

Aadhaar has huge potential to bring about financial inclusion in large parts of the society which has remained marginalized and devoid of benefits so far.

The ability of Aadhaar to uniquely identify an individual electronically makes it a valuable tool in administration of Government schemes and benefits, and a natural financial address on the basis of which funds can be transferred directly into a beneficiaries linked account. The beneficiary can link their Aadhaar number to their bank account to receive the payments seamlessly and would also have the option of changing this at any point in time. Aadhaar enabled bank accounts bring financial access and affordability to millions of residents who are presently excluded from formal financial systems. An Aadhaar enabled bank account will also help residents make cheaper, faster electronic transactions and remittances in the form of micropayments. The solution will enable universal access to their account from any bank or BC, and through any mobile device, enabling residents to access payments on the move. Regular, affordable access to banking services would also give the poor a means of keeping their

[6] Aadhaar Seeding Protocol http://uidai.gov.in/images/aadhaar_seeding_june_2015_v1.1.pdf

money safe — a convenience that has long been available to the middle class would now be accessible to the rural and urban poor.

****** end of the document ******