AADHAAR TECHNOLOGY STRATEGY

Ecosystem, Technology, & Governance

UIDAI Technology Center

March 2014

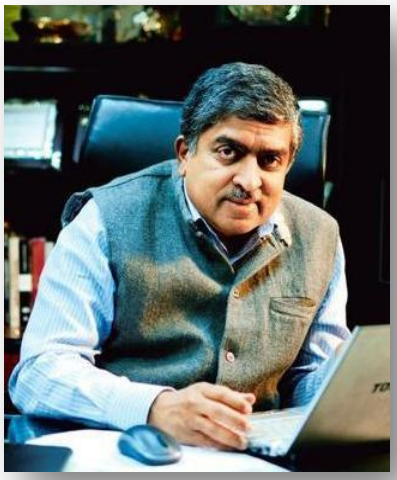
AADHAAR TECHNOLOGY STRATEGY

Ecosystem, Technology and Governance

MARCH 2014

UNIQUE IDENTIFICATION AUTHORITY OF INDIA
PLANNING COMMISSION, GOVERNMENT OF INDIA
JEEVAN BHARATI BUILDING, CONNAUGHT CIRCUS, NEW DELHI – 110001

Message from Chairman



UIDAI has the vision of empowering every resident of India with a unique identity and providing a digital platform to authenticate anytime anywhere. The Aadhaar system is built on a sound strategy and a strong technology backbone and has evolved into a vital digital infrastructure. Meticulous planning and execution enabled the program to be launched ahead of plan in Sept 2010 and reach the kind of scale that was never achieved in any biometric identity system in the world.

UIDAI created an ecosystem of partners for the various key components of the project and integrated them all onto a common technology backbone using open standards. Aadhaar technology system was able to succeed due to its core principles - openness, vendor-neutrality, security, and data analytics. In the absence of digital privacy laws, UIDAI took it upon itself to implement rigorous standards and measures to ensure data privacy and security. Apart from generating 60 crore (600million) Aadhaars in 4 years through this approach, the Aadhaar platform is now integrated into the financial systems of NPCI and banks, taking India towards the goal of total financial inclusion.

Documenting of the design and implementation of the Aadhaar technology, which evolved over a period of four years, was as onerous as building the system itself. The UIDAI Technology Centre has done a commendable job in compiling white papers on technology strategy, application features, and architecture. These documents place the Aadhaar system on a firm foundation and also serve as the beacons for many eGovernance projects in India and across the world.

My hearty congratulations to the UIDAI technology team!

Nandan Nilekani
Chairman, UIDAI

Message from Director General

Aadhaar project, under the Planning Commission, Government of India, is an initiative to provide a unique identification number to every resident that can be leveraged by the residents to access various services and benefits. Uniqueness of Aadhaar identity allows elimination of fake and duplicate accounts, and online authentication provides a mechanism for paperless, electronic and instantaneous verification of identity, anytime anywhere. Aadhaar platform can be utilized by various Governmental, public, and private sector agencies to efficiently deliver services to residents.

By its very nature, the Aadhaar system needed a strong technology foundation. Appropriately, the Technology Centre was the first unit of UIDAI to start functioning in 2009 in Bangalore. UIDAI technology team was able to develop the required applications and successfully generate the first Aadhaar number within a year of its formation. The architecture was rigorously tested and validated through a series of 'Proof of Concept' studies. Aadhaar generation was commenced in August 2010 and the first Aadhaar letter was formally handed over to a resident at Nandurbar in Maharashtra on 29 September 2010. Subsequently Authentication and e-KYC services were also launched.

In the course of attaining the milestone of 60 crore (600 million), the Aadhaar technology backend has become the largest biometric identity repository in the world and the first to provide an online, anytime anywhere, multi-factor authentication service. A strong technology foundation based on open architecture enabled the rapid evolution of the Aadhaar system. It was important to document all aspects of Aadhaar technology and make it available in public domain. The three white papers published by the UIDAI Technology Centre fulfil this need.

I sincerely appreciate the efforts of our technology team in publishing these.

Vijay Madan
Director General, UIDAI

From the Editor's Desk

'Aadhaar' is undoubtedly one of the most important Projects rolled out by Government of India. Ambitious, one-of-a-kind and a game-changer, 'Aadhaar' is on the path of delivery to every Indian resident, a 'national identity' and triggering thereby the much desired governance system based on social inclusion, transparency & accountability.

Considering India's population of 121 crores, it is obviously a highly ambitious project. Any Project of this magnitude prospers and grows based on the contributions from the people associated with it. Unique Identification Authority of India (UIDAI) has been blessed in this regard. Many outstanding people from both Private and Government sectors, spanning the domains of - Administration, Biometrics, Project Management, Law, Technology and Finance, to name a few - have come together and dedicated their talent, time and knowledge, besides the much needed passion & commitment.

UIDAI has also been led by competent people like Shri Nandan Nilekani, as its Chairman, Shri Ram Sewak Sharma, as its first Director General and Dr Vijay Madan, who succeeded him a year back. Shri Nilekani has provided both visionary and charismatic leadership to the Organisation as its Founding Chairman. With his experience of building one of India's internationally recognised I.T. Companies; besides his association with both State & Union Governments in different advisory capacities, he was an appropriate choice to establish and lead an organisation like UIDAI that called for an understanding of technology and a commitment to social inclusion. The yeoman services rendered by the first Director General, Shri R.S Sharma are recalled with fondness. A man of boundless energy and dedication, Shri Sharma with his attention to detail and sharp technical knowledge, ensured that the Project got the right kick-start and maintained momentum in its formative years. Dr Madan has been the perfect foil to the Chairman besides being an able successor as the current Director General. He has been able to expand the horizon of the Organisation by steering it to the next growth trajectory for quicker delivery of Aadhaar and its deployment for people-centric Applications. His focus also has

been on knitting together different components into a single and synergetic unit for this purpose.

UIDAI has always believed in documentation and sharing of information with public. Technology & processes that characterise UIDAI needed to be brought within the public domain as a matter of transparency, as also to elicit debate and discourse. Towards this end, the White Papers have been in the making for a while. I acknowledge the contributions of Shri Srikanth Nadhamuni, Dr Pramod Varma, Shri Sanjay Jain and Dr Vivek Raghavan in writing the papers. Our ADGs at the Tech Centre too have been actively involved in writing and reviewing them. The contributions of Shri Rajendra Kumar, Shri Sudhir Narayana, Shri Venkat Rao and Shri Anup Kumar are appreciated in particular.

The writers and reviewers have not lost sight of the need for a simple & straight language while putting together the highly technical and procedurally rigorous content of the Project. They have done a commendable job. Further, these documents are a manifestation of an intensely cerebral and immensely taxing effort put in by a band of dedicated domain experts who worked with the UIDAI's Tech Centre at different stages of its evolution. There are many, but some who definitely need a mention are Srikanth Nadhamuni, Raj Mashruwala, Pramod Varma, Sanjay Jain, Vivek Raghavan, and Jagdish Babu. Our colleagues including Dy. Directors General, Asst. Directors General and others serving UIDAI's cause at the Headquarters, Regional Offices and Technology Centre have contributed in multiple ways to the evolution of technology, processes & procedures and the compilation of this document. I beg pardon for not mentioning them by name. All of them are gratefully acknowledged.

It is a matter of pride and pleasure that these are getting published as the UIDAI reaches the hallmark of 60 crore Aadhaars well ahead of the targeted date and gears up to provide identification to the other half of the nation.

Ashok Dalwai
Deputy Director General, UIDAI
Technology Centre, Bengaluru

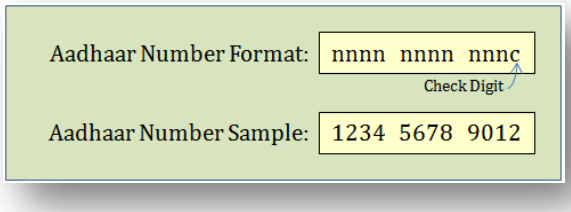
Table of Contents

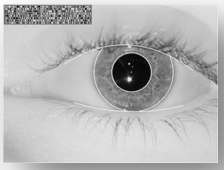
Table of Abbreviations

ABIS	Automated Biometric Identification System
API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BFD	Best Finger Detection
BI	Business Intelligence
BPL	Below Poverty Line
BSP	Biometric Service Provider
CIDR	Central Identity Data Repository
DDSVP	Demographic Data Standards & Verification Process
DoB	Date of Birth
EA	Enrolment Agency
ICDS	Integrated Child Development Services Scheme
JSY	Janani Suraksha Yojana
KYC	Know Your Customer
MNREGS	Mahatma Gandhi National Rural Employment Guarantee Scheme
OTP	One Time Pin
PDS	Public Distribution System
PID	Personal Identity Data
PII	Personal Identity Information (Personally Identifiable Information)
PoA	Proof of Address
PoI	Proof of Identity
RSBY	Rashtriya Swasthya Bima Yojna
SSA	Sarva Shiksha Abhiyan
UIDAI	Unique Identification Authority of India

Executive Summary

There has been a lot of focus on infrastructure projects in India such as roads, metros, ports, etc. As India moves towards large scale e-Governance adoption, a soft infrastructure for Government service delivery, agencies implementing these need to ensure efficiency and accountability across those systems. A national ID system such as Aadhaar is a very important platform that can improve the efficiency and transparency of various e-Governance initiatives in the areas of food security (PDS), jobs (MNREGA), health (JSY) etc.





The focus of Aadhaar [1] [2] is to issue a unique 12 digit number to every Indian resident and thereby create an Identity Platform that can be used by various departments of the Government as well as public and private sector entities and NGOs. Aadhaar provides an online authentication system which can be used to verify the identity of residents electronically during service delivery [3] [4]. This fast, anytime, anywhere verification of resident's identity can bring about accountability and efficiency in the various government benefit schemes as well as other private sector uses. UIDAI also provides an e-KYC service [5] - an instant, electronic, non-repudiable proof of identity and proof of address which can be used for KYC checks in banking, telecom and other sectors.

In order to maintain uniqueness (meaning one person gets one and only one Aadhaar) the biometrics of the resident need to be collected. The UIDAI Biometric Standards Committee recommended [6] that 10 fingerprints, 2 irises, and facial photo of the resident be collected. Several proof–of-concept studies were carried

out to ensure that the biometric technology was capable of enrolling and authenticating the entire population.

Since Aadhaar system has to enrol more than one billion people, UIDAI needed to create an ecosystem of partners such as Registrars, Enrolment Agencies (EAs), certification agencies, operators, letter printers, etc. to implement various components of the project on the ground based on UIDAI defined technology standards and processes.

Due to the complexity of creating a national ID database over a billion people, a sophisticated technology backbone was needed. UIDAI Technology Centre was setup in 2009 in Bangalore to develop and deploy the initial Aadhaar application and set up CIDR (Central Identity Data Repository). For the entire system to scale to a billion residents, an open source and open standards approach was adopted. To ensure privacy and security of the residents' data, in the absence of a data privacy law in India, stringent security and data privacy policies were established and enforced by UIDAI.

To provide real-time updates on the Aadhaar project to all its stakeholders a Business Intelligence (BI) and Analytics platform was developed that provides dedicated web portals to residents, registrars, and other stakeholders. This transparent, electronic and real-time flow of information and analytics to all stakeholders resulted in continuous improvement of all parts of the Aadhaar system.

The Aadhaar project has issued more than 600 million (60crore) Aadhaar numbers within 4 years of its national launch. The biometric systems both on the enrolment and authentication side are working at high levels of accuracy. The authentication service is fully functional, supporting fingerprint, iris, and OTP authentication and is currently being used successfully by several agencies as part of their service delivery to residents. The e-KYC service is used by agencies such as banks to make "Know Your Customer" (KYC) process convenient and paperless. There is huge interest in the resident population to enrol for Aadhaar, resulting in about 10-15

lakh Aadhaar enrolments each day. With the rapid adoption of Aadhaar authentication and e-KYC services by the various government schemes, financial, telecom and other sectors, it is expected that tens of millions of Aadhaar transactions will take place every day making it one of the most successful e-Governance initiatives taken up.

Readers should read the following documents along with this document so as to get a complete understanding of Aadhaar strategy, application functionality, and its technology architecture.

1. UIDAI Strategy Document [1]
2. Aadhaar Product Document [7]
3. Aadhaar Technology Architecture [8]

1 Introduction

Without a bridge, the shore on the other side of a river can seem far indeed. Infrastructure – roads and rail, bridges and electricity, plumbing, sewage systems – enables access and connection, the efficient movement of people and capital, and the growth of markets. Investments in infrastructure boost economic growth and productivity, while providing significant positive spill over into areas such as energy efficiency and public health.

In the last few decades a new kind of soft infrastructure has emerged, which is based on computers, electronic networks and data storage. It has enabled revolutionary new technologies, such as the Internet, mobile telephone networks and high-speed voice & data networks to flourish. These technologies have become essential tools of development and growth, contributing to global integration and enhancing the effectiveness, efficiency, and transparency of the public and private sector. In India, several applications have been built on this new infrastructure. The railway reservation system for instance, has made the purchase of train tickets a lot more convenient; the core banking system and ATM networks have made access to banking a lot easier. India has also been a significant beneficiary of high speed intercontinental electronic networks that have allowed IT and other services to be provided to the rest of the world.

This soft infrastructure is taken into consideration while building Aadhaar identity platform – a system that can uniquely identify residents of a country with anytime anywhere usage. In the Indian context, such a system helps in bridging critical services for the poor. In a country where the government has several benefit schemes targeting the poor, a national identity system can significantly increase the effectiveness and efficiency of service delivery.

National ID system does not eliminate other application specific IDs. Instead it is used as the "breeder" document that can be used along with other program specific IDs. For example, low income medical insurance program will require national ID plus income documentation to issue medical insurance card. Without good reliable breeder document, every government program has to either create its own robust system to establish uniqueness and universality or risk leakage and duplication.

1.1 Aadhaar – Unique Identity System

National Identity systems are used by many governments to identify their residents, in-order to deliver welfare benefits, health care, financial services and ensure border control.

There is no common national ID system in India that covers all residents, but there are several separate databases of information such as the PAN (Permanent Account Number) card, EPIC (Electoral Photo Identity Card), Ration Card, etc. that represent subsets of the population and are specific to certain applications, such as for the levy of income-tax, for voter registration, and for food distribution. The core idea of the Aadhaar project is the issuance of a Unique Identification (Aadhaar) number to all "residents" of India so they can use it for multiple schemes and purposes. This is critical considering large numbers of people migrate from one part of India to another for education and work.

A large number of Indians, especially across rural India, lack identity documents through which they can apply to government benefit schemes. While many may have certain documents such as a ration card or an MNREGA card, these are 'limited' identities, valid only in the state/context for which they are issued; these are usually not valid for other government services, or when the individual migrates to other geographical areas.

An inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals

with services. But, till date, there remains no nationally accepted, verifiable identity number that both residents and agencies can use with ease and confidence.

As a result, every time individuals try to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual. Such duplication of efforts due to 'identity silos' increase overall cost of identity verification and cause inconvenience. This is especially hard for India's poor and underprivileged residents, who usually lack documentation and find it difficult to avail various services and benefits.

There are clearly immense benefits from a mechanism that uniquely identifies a person and ensures instant identity verification. The need to prove one's identity only once will bring down transaction costs. A clear identity number can transform the delivery of social welfare programs by making them more inclusive of those communities now cut off from such benefits due to their lack of identification. It also enables the government to shift from indirect to direct benefit delivery by directly reaching out to the intended beneficiaries. A single universal identity number is also useful in eliminating fraud and duplicate identities, since individuals can no longer be able to represent themselves differently to different agencies. This results in significant savings to the state exchequer.

Indians are increasingly migrating in large numbers in search of jobs and better prospects -- it is estimated that more than 300 million migrant workers have left their villages/cities in search of permanent or seasonal work elsewhere. Hence, it is important for residents to be able to identify themselves anywhere in the country using a common nationally valid identity document, so that they can access various services and schemes that they are entitled to.

A national ID that is portable and universally accepted by governments, banks, telecom operators and other key institutions is hugely beneficial to the residents of the country.

There are several key characteristics of such a system that are essential in order for it to be useful:

- The ID should be available to all residents of the country.
- The system should ensure that each resident gets only one ID, hence making it unique.
- The system should ensure that only the owner of the ID can use the ID to make a transaction.
- The system should be capable of electronically authenticating residents so that the government/private service delivery systems can ascertain identity of their customers.
- Lastly, authentication should be available online anytime, anywhere, so that the ID is recognized across the country over networks, thereby improving service delivery.

1.2 History of National ID in India

The Government of India undertook an effort to provide a clear identity to its residents first in 1993, with the issue of photo identity cards by the Election Commission. Subsequently, in 2003, the Indian Government approved the Multipurpose National Identity Card (MNIC).

The Unique Identification Authority of India (UIDAI) was established in February 2009, attached to the Planning Commission. The mission of the UIDAI is to issue a Unique Identification number (Aadhaar number) to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way [2]. The UIDAI's approach keeps in mind the lessons from the government's previous efforts at issuing identity.

1.3 How Identity Systems Work

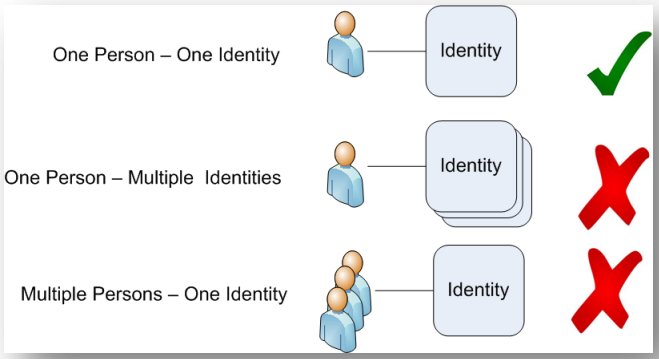
A national identity platform requires a database of unique residents. In the past, many central and state projects have attempted to create identity systems for the people under specific schemes or jurisdiction.

There have been several problems that have plagued these identity systems:

1) **Duplicate Identities**: Where the same resident gets multiple identities in the system.
2) **Fake Identities**: Identities created using fake documents of people that actually do not exist or identities of people who no longer exist.

These forms of identity fraud are largely due to the desire to illegitimately capture a larger share of resources that flow through public benefit systems – such as PDS, LPG, kerosene etc. In order to effectively address the above problems, reforms must be systemic, and there are three conditions that an identity system must satisfy:

1. Each identity in the system must be linked to a *real* eligible person
2. Each identity must link to *one and only one* eligible person in the system
3. Multiple identities should not be issued to one person



How does one ensure that only unique identities are created, without duplicate and fake identities? Identity systems that rely only on demographic fields (e.g. name, DOB, address) and personal reference checks are identity surrogates and vulnerable to forgery, falsification, theft, loss, and other corruption. Since biometric markers such as fingerprints, iris patterns etc. are unique to people, they can be used to ensure uniqueness.

Identity systems that support authentication typically answer the question, '*Are you who you say you are?*'

They do so by using different factors:

- "*What you know*" – user ID/password, PIN, mother's maiden name, etc.
- "*What you have*" – a token such as card, hardware dongle, mobile phone, etc.
- "*What you are*" – biometric markers such as face, fingerprint, iris, voice etc.

Biometric factors can give a high quality of authentication assurance in an identity system without having to issue and manage expensive tokens to large population. In India, where reliable and clean identity databases do not exist, usage of biometrics is the most suitable for carrying out de-duplication. It is hence necessary to enrol all residents along with their biometrics and build a clean database for the purposes of creating a national unique identity system.

1.4 Features of Aadhaar

UIDAI only provides identity – The UIDAI's purview is limited to the issuance of unique identification (Aadhaar) numbers linked to a person's demographic and biometric information. The UID number (Aadhaar number) only guarantees identity, not rights, benefits or entitlements.

Aadhaar number proves identity, not citizenship – As per UIDAI's mandate [2], all legal residents (anyone legally residing in India) in the country can be issued Aadhaar number. Possession of Aadhaar number is merely a proof of identity and does not confer citizenship.

A pro-poor approach – The UIDAI envisions full enrolment of residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars (such as State Governments) that the UIDAI partners with help bring large numbers of the poor and underprivileged into the Aadhaar system. Providing token-less (no cards or other physical tokens), online, anytime anywhere authentication improves service delivery to the poor.

Enrolment of residents with proper verification – Existing identity databases in India are fraught with problems of fraud due to duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the UIDAI enrols residents into

its database with proper verification of their demographic information based on the recommendations of the DDSVP Committee headed by Shri N. Vittal [9]. This ensures that the data collected is clean from the start of the program. However, much of the poor and underserved population lack identity documents and Aadhaar may be the first form of identification they have access to. The introducer model proposed by the DDSVP Committee allows UIDAI to ensure that the procedures do not become a barrier for enrolling the poor.

A partnership model – UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI is the regulatory authority managing a Central Identity Data Repository (CIDR), which will issue Aadhaar numbers, update resident information, and authenticate the identity of residents as required. UIDAI partners with agencies such as central and state departments who are the 'Registrars' for the UIDAI. Registrars conduct the enrolment camps using UIDAI software and procedures, upload the encrypted enrolment data to the CIDR to de-duplicate resident information, and help seed the Aadhaar number into their beneficiary databases.

Enrolment is not mandated – Aadhaar strategy uses a demand-driven model, where the benefits and services that are linked to the Aadhaar number ensure demand for the number. This will not however, preclude governments or Registrars from mandating enrolment.

UIDAI issues a number, not a card – The UIDAI's role is limited to issuing the number which is communicated to the resident through a letter. This number may be printed on the document/card that is issued by various usage agencies.

Aadhaar number does not contain any intelligence – Embedding personal data into identity numbers makes them susceptible to fraud and discrimination. Aadhaar number is a random number making it purely a national identity that can be used across the country.

UIDAI only collects minimal information – Aadhaar enrolment only seeks the following demographic and biometric information:

1. Name

2. Date of birth (or Age)
3. Gender
4. Address
5. Mobile Number and Email (optional)
6. Ten fingerprints, two iris scans, and photograph
7. For children under five years old, Aadhaar number and name of the guardian (Father/Mother/Guardian)

Process to ensure no duplicates – Registrars send the applicant's encrypted data packet to the UIDAI data centres for de-duplication. Aadhaar enrolment system performs a search on key demographic fields and on the biometrics for each new enrolment, to ensure uniqueness.

Process to keep data up to date – Incentives in the Aadhaar system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the Aadhaar system ensures that residents have only one chance to be in the database, individuals are incentivized to provide accurate data. This incentive becomes especially powerful as benefits and entitlements are linked to the Aadhaar number. Regular usage of identity across many services naturally incentivizes the resident to keep Aadhaar system up to date.

Online authentication – UIDAI offers a strong form of online authentication. When residents wanting to avail a service require identity/address verification, agencies can compare demographic and biometric information of the resident with the record stored in the central database.

Explicit resident consented e-KYC – A balance between 'privacy and purpose' is critical to ensure convenience of online identity is balanced with the requirement to protect resident identity data. Aadhaar authentication only responds with a 'Yes' or 'No' response and no resident data is sent back. Aadhaar e-KYC service allows resident to authorize UIDAI to share electronic version of their Aadhaar letter. For every Aadhaar e-KYC request, only after successful resident authentication, demographic and photo data is shared in electronic format (via biometric/OTP

authentication resident explicitly authorizes UIDAI to share electronic version of Aadhaar letter instead of sharing physical photocopies). Resident authorization is NOT used for multiple e-KYC transactions, instead, every time agencies require electronic version of Aadhaar letter data for KYC purposes, resident must authorize the agency.

Technology undergirds the UIDAI system – Technology systems have a major role across the UIDAI infrastructure. Large scale biometric de-duplication, online authentication, data security, analytics, etc require well designed, secure, and scalable systems.

1.5 Opportunity to Reengineer

Via its features and open APIs, Aadhaar system is designed to enable process reengineering in various service delivery systems. While Aadhaar system itself is a minimalistic unique identity platform, innovations using Aadhaar will happen in other systems that take advantage of Aadhaar. Agencies implementing various service and benefit delivery programs should look for opportunities to reengineer those programs using Aadhaar.

Instead of imitating current paper processes in electronic form, applications should look to embrace Aadhaar for its uniqueness and permanency, go fully online, adopt mobile as the primary interface, and use Aadhaar authentication and e-KYC services to transform the processes completely. While making the projects efficient and transparent, such transformations can offer a wider choice and no/low touch point to residents. It is critical that e-Governance projects are aligned with larger trends and are designed for next decade rather than past.

It is also essential that whenever large scale changes are done, solutions must naturally cater to the incentives of the "participants" (residents, agencies, operators, etc) within those systems. In any transformational e-Governance project, if design is not aligned to natural incentives of residents, Government, and partners, there is a high chance that the project will fail.

1.6 Role of Biometrics in Aadhaar

Any human physiological or behavioural characteristic could be used as a biometric provided it has the following desirable properties:

- **Universality**: Every person should have the characteristic.
- **Uniqueness**: No two persons should have the same characteristic.
- **Permanence**: The characteristic should not completely vary with time.
- **Collectability**: The characteristic should be quantitatively measurable.

Later chapter describes the role of biometrics within Aadhaar enrolment and authentication in detail.

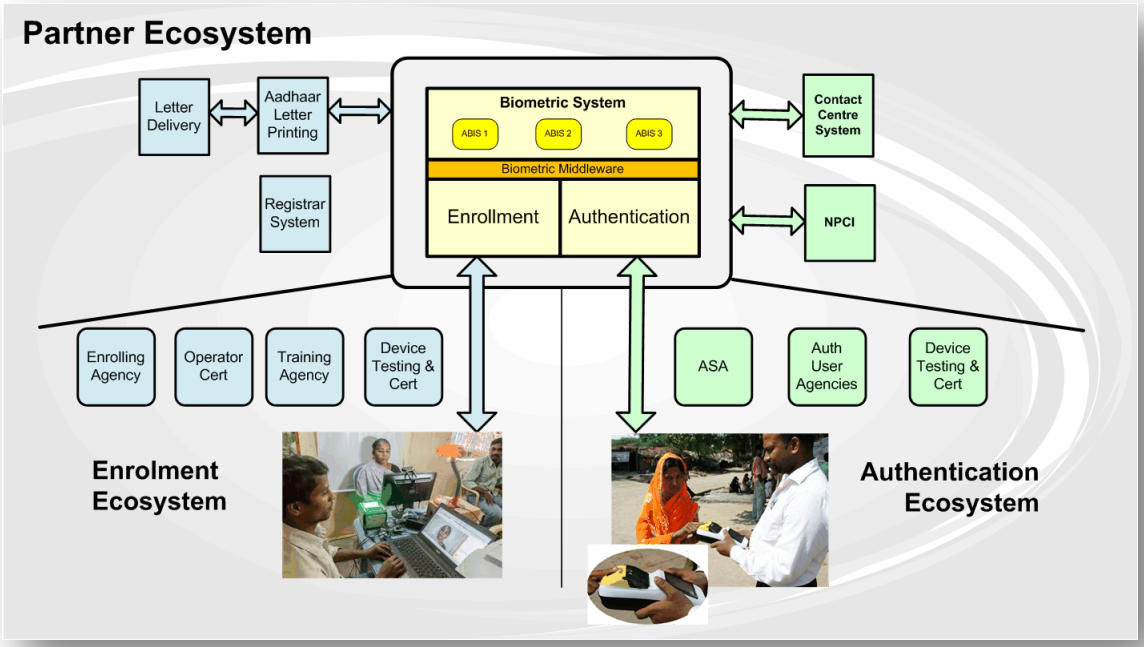
2 Building a Scalable Program

How do you implement a program for 1.2 billion people to create the largest biometric identity system in the world? National identity projects are run in several countries by a single monolithic agency whose mandate it is to enrol its population. It was evident from the very beginning that given India's diversity – urban/rural, rich/poor, literate/illiterate etc. - Aadhaar system would be best implemented by a set of cooperating partners or stakeholders.

Key design concepts that help a large project of this nature to succeed are:

- Keep the front-end field processing of enrolments as easy as possible, and move the intelligence to the backend.
- Do not make the front-end restrictive, provide a choice of multiple enrolling agencies, and build in the idea of enrolling anywhere in India.
- Build robust BI & Analytics platform for continuous improvement, so that improvements and decision making can be based on data.

Given the federal nature of the governance with strong State Governments that implement many of the flagship schemes, it was important to enlist the State Governments as Registrars for enrolling the residents of their respective states. The project needed Enrolment Agencies (EAs) to actually perform field operations on behalf of these registrars. These EAs needed to procure standard enrolment kits. It was important to create a cadre of trained enrolment operators and supervisors who work for these agencies. This, in turn, required training and certification agencies. The ecosystem also needed device manufacturers and suppliers who would provide Aadhaar compliant devices for enrolment and authentication; this in turn needed a testing and certification agency.



It was clear from the very beginning that a project of this scale could not be implemented by a single agency. UIDAI needed an ecosystem of cooperating partners from Government departments, private sector players, and NGOs to help implement the project. Such ecosystem approach also necessitated that the interfaces between these partners and systems were well defined and standardized. UIDAI also needed to build a technology backbone that would hold together this partner ecosystem.

At the data centres where the enrolments were processed, UIDAI needed a set of suppliers to provide pieces of the Aadhaar backend system, most importantly, a set of Biometric Service Providers (BSPs) to provide multi-modal biometric de-duplication software solution that can de-duplicate the incoming enrolment requests and ensure that they are truly unique. In addition, UIDAI needed one or more agencies for application software development, 24x7 data centre operations, and security monitoring.

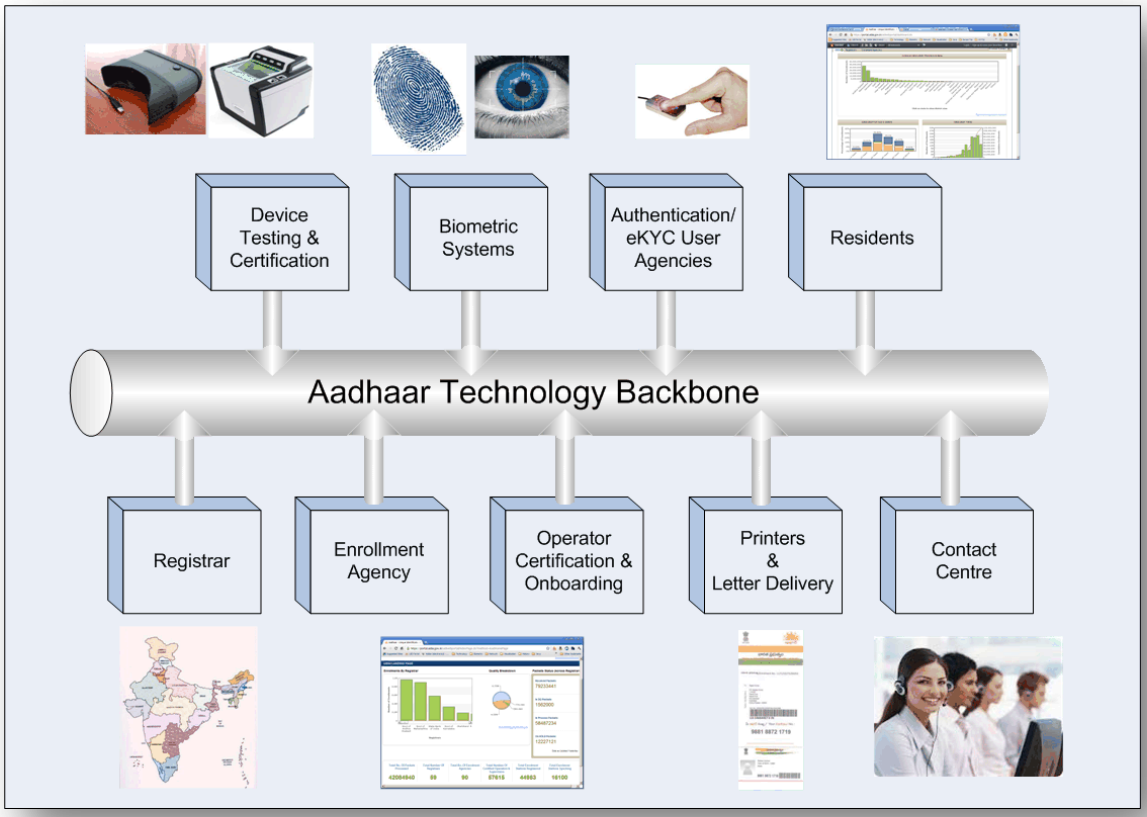
2.1 Aadhaar Technology Backbone

The mammoth nature of the project and its ecosystem of partners and stakeholders is a challenge to integrate. The various partners need to be supported in their activities and tightly integrated into the Aadhaar technology 'backbone' in order to ensure seamless integration and smooth service delivery to residents. This would not have been possible by simply deploying an army of employees. This needed a sophisticated technology backbone that integrates the partner systems, automate various processes and reduce/eliminate manual intervention through open technology and process standards.

Given below are ecosystem integrations into the Aadhaar Technology backbone:

1) **Contact Centre Integration**: The Aadhaar Contact Centre handles phone support on a toll-free phone line that residents can call if they have a problem that they want to resolve. The contact centre support personnel need online but secure access to the appropriate parts of system to handle the specific problem that the resident was facing – such as an 'Aadhaar letter not delivered'. This contact centre integration has been accomplished technically using specific APIs (Application Programming Interface) with authentication and access control. UIDAI currently works with multiple contact centre providers all integrating using common technology and processes.
2) **Biometric Systems**: Automated Biometric Identification Systems (ABIS) software had to be tightly integrated with the Aadhaar enrolment server in order to perform trillions of de-duplications each day. A multi-ABIS strategy mandated multiple (three at present) ABIS software solutions to be used and operated simultaneously. This multi-ABIS strategy is to de-risk the project in the eventuality when an ABIS solution does not meet the accuracy and performance requirements. Aadhaar system has achieved this by tight integration through the ABIS APIs [10] that stipulate to the ABIS solution providers even before procurement so that an ABIS solution can be replaced without affecting rest of the Aadhaar system.
3) **Operator Certification and activation**: Operators who perform enrolments are trained and certified in order to ensure high quality enrolments across the country. Typically, the operators are trained by EAs and take a test which is administered by approved certification agencies. Test results are updated in

the Aadhaar system so that when the EA logged in to the Aadhaar system via partner portal, they could ascertain the eligibility of the operators such as having their own Aadhaar number, certification etc. This entire process is automated and integrated into the Aadhaar backend system so there is no manual intervention. Currently there are over 100,000 certified operators in the ecosystem.



4) **Partner Portals**: Key Aadhaar partners such as Registrars, Enrolling agencies, Authentication & e-KYC user agencies get their own 'cubby-hole' in the Aadhaar system to monitor their own work and progress. Partner portals are created for this specific reason. The Registrar-facing part of portal gives information on the number of enrolments, tabulated by EAs. They can break down these numbers by district and evaluate the progress of their enrolments. Similarly, EA-facing part of portal is created for EAs to track how each of their operators is performing. They get their own dashboard to see the number of enrolment

stations, operators that are active, the number of enrolments conducted by them and aggregate analytics such as the average number of enrolments per station per day.

2.2 Use of Open Source & Open Architecture

Entire technology architecture behind Aadhaar is based on principles of openness, linear scalability, strong security, and most importantly vendor neutrality.

Aadhaar technology backbone is built using the following architecture principles:

- **Open architecture** – Building Aadhaar system with true openness meant use of open source and standards to ensure interoperability; platform approach with open APIs to allow the ecosystem to build on top of Aadhaar APIs; vendor neutrality across the application components using open and standard interfaces; and identity system designed to work with any device, any form factor, and any network.

- **Design for scale** – Aadhaar system is expected issue 1.2+ billion identities for the current residents and continues to grow as the resident population expands. Since every new enrolment requires biometric de-duplication across the entire system, every component needs to scale to very large volumes. This meant system must handle hundreds of millions of transactions across billions of records doing hundreds of trillions of biometric matches every day! In addition all online services such as Aadhaar authentication, e-KYC service, and update service must work with high availability and sub-second performance. Network and data centre load balancing and multi-location distributed architecture for horizontal scale are critical to such massive scalability.

All application components are built using open source components and open standards. Aadhaar software currently runs across two of the data centres within India managed by UIDAI and handles 1 million enrolments a day and at the peak doing about 600 trillion biometric matches a day. Current system already has

about 4 PB (4000 Terabytes) of raw data and continues grow as new enrolments come in. Aadhaar Authentication service is built to handle 100 million authentications a day across both the data centres in an active-active fashion and is benchmarked to provide sub-second response time.

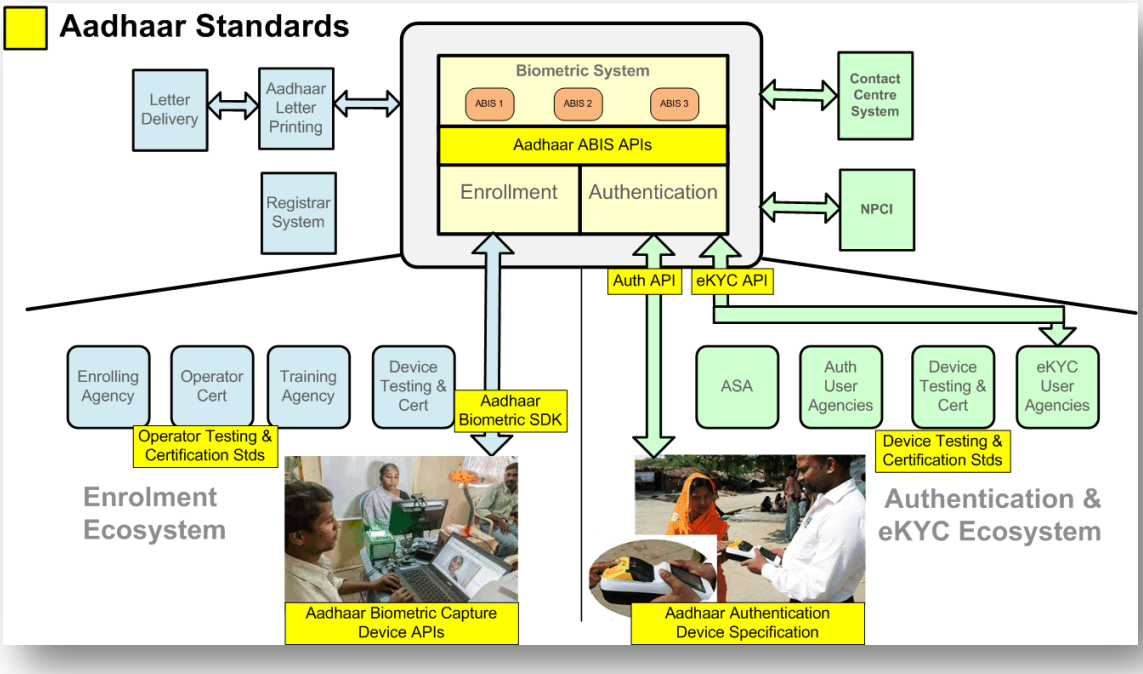
2.3 Process & Technology Standards

There are three key reasons why the standards approach is imperative to the success of Aadhaar.

Process Standards: When the system is constructed with a set of cooperating partners, it is a challenge to ensure uniform quality of enrolment data, processing and hence output. Standardization of the enrolment elements – the devices that capture the data such as fingerprints and iris, and the client software that is used to capture the demographic and biometric information – was absolutely essential.

Interoperability: Aadhaar system consists of various partners whose systems had to be integrated for seamless operations. This implied that the interfaces between the various sub-systems needed to be defined very carefully, in a vendor neutral way, and in exacting detail. Standard APIs were defined for each of the partner systems to be integrated to the Aadhaar system.

Vendor Neutrality: A key infrastructure such as a national identity system should not be locked into specific vendor proprietary technologies and components. So while every attempt was made to use open-source components, in places where only proprietary technologies were available/suitable, it was important that they adhered to open standards and interfaces, such that these proprietary components could be replaced if necessary without sacrificing the integrity or performance of the entire system.



Standards adopted by the Aadhaar system largely fall under the following buckets:

Enrolment software and device standards

The Aadhaar biometric enrolment software uses national and international standards where available, for individual data elements to ensure interoperability with different software vendors. For instance, the biometric data is required to conform to ISO standards, with no extensions, to ensure that processing could be done by in a vendor-neutral way. Following are key specifications that are available for enrolment.

- **CBEFF** - The Common Biometric Exchange Formats Framework (CBEFF) is used to define a standard way to combine the all biometric data of a resident into common data structure.
- **Transliteration API** - A transliteration API (in Java) to allow multiple vendors to provide transliteration services, to help the operators enter the demographic data in 2 languages simultaneously. This allows the Aadhaar system to always choose the best option for each language.

- **Biometric SDK API** - Each biometric vendor is required to provide a library for the purpose of biometric data processing – quality checks, format conversion, segmentation, local matching, etc. - which allows the enrolment client software to perform various checks at the time of capture itself. To ensure vendor neutrality, this has been standardized and published [11].
- **Biometric Capture Device API** - There being no device interface standards available, a standard interface has been defined and all biometric device vendors are required to provide a device driver [12] based on this API. This has allowed the enrolment client to be developed completely independent of the devices. This has also allowed for the building of various test harnesses and other tools for device certification. Conformance to this interface is a mandatory requirement for certifying that the device works with the Aadhaar enrolment station. This standardized plug-n-play approach has had the effect of creating an open market for biometric devices of multiple vendors thereby bringing prices down.
- **GPS Interface** - The GPS device used at enrolment station must conform to the NMEA-0183 standard. This allows the enrolment client software to be developed without considering the specific GPS device used in the field.
- **Scanner Interface** - The Aadhaar enrolment client requires a flatbed scanner for scanning supporting documents used for enrolment data verification. UIDAI has mandated that all scanners used in the program must support industry standard TWAIN interface.

Enrolment process standards

The Aadhaar enrolment process requires that all enrolment operators and supervisors to be Aadhaar holders, trained, certified, and able to authenticate themselves for each enrolment. This ensures all enrolments are traceable.

Further, the process requires that all enrolment stations conform to certain standards, and have various peripherals that conform to standards. For instance, the biometric capture devices must be certified by the STQC and compliant to Aadhaar Biometric Capture Device API specification [12]. Every enrolment station includes the use of a second, resident facing screen so that the resident can verify the data being entered by the operator. The enrolment process also specifies the form that is used to capture the data, options for proof documents, the process to verify these documents, and certain exception conditions.

Finally, the enrolment process requires that the operators use the standard enrolment client software provided by the UIDAI. This ensures that training and process materials can be created centrally, and that all operators across the country can provide a consistent experience to the residents. The entire set of process documents are published by the UIDAI on its website, and revised based on feedback ensuring continuous improvement.

Authentication software and device standards

The UIDAI has published specifications for a common authentication API [13]. This allows various developers to build authentication applications for their domain, on their preferred platform. Following are key specifications that are available for authentication and e-KYC.

- **Authentication, e-KYC, and supporting APIs** - Standard API specifications [13] [14] [15] [16] are provided for all applications to use and are published on UIDAI website. All applications using Aadhaar online services must adhere to these specifications.
- **Sensor Specification & Certification** - The UIDAI conducted extensive field studies on authentication, with various devices [17]. Based on these studies, the UIDAI identified several devices that are able to reach an acceptable accuracy for authentication, as well as characteristics of these devices. The UIDAI and STQC have created certification scheme based on

device features. Continuous field testing and certification process allow newer device technologies to be certified thereby benefiting the user agencies in adopting latest technologies.

2.4 Authentication & Application Ecosystem

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

Combination of Aadhaar Number and biometrics ("*who you are*" factor) deliver online authentication without needing a token (such as a smartcard). OTP authentication allows AUAs to verify the possession of the mobile phone ("*what you have*" factor) by sending the One-Time-Pin to resident's mobile phone and re-verifying it. Aadhaar authentication provides multi-factor authentication using resident fingerprints, iris, and mobile phone. By combining one or more factors, authentication of the resident could be strengthened. In addition, Authentication User Agency (AUA) specific factors such as ATM cards or smart cards or passwords may also be used in conjunction with Aadhaar authentication to further strengthen user authentication.

UIDAI has published open APIs for authentication [13] and related services for application developers and Authentication User Agencies [4]. Designing the Aadhaar system as pure identity platform allows clear separation of duties and leaves "usage" of identity to various applications built on top of the Aadhaar platform. Such ecosystem approach allows large developer ecosystem to innovate and transform service delivery by building applications on top of Aadhaar platform.

2.5 Business Intelligence & Continuous Improvement

A strategic initiative adopted by the UIDAI from the design stage has been the extensive usage of "Analytics and Reporting" to aid operations. This has been

documented in detail in a paper entitled "*Analytics - Empowering Operations – The UIDAI Experience*" [18].

Reporting is the process of sharing data related to an organization with key stakeholders. Analytics is the structured process of analysing this data to derive insights that help operations. The UIDAI's experience as well as emerging academic research indicates that Analytics and Reporting deliver concrete benefits to end-to-end operations. These benefits span the tactical, operational and strategic levels, helping move decision making from "intuition based" to "data based":

1. Creating information conduits that provide end-to-end integrated visibility to management across the entire ecosystem.
2. Having a common language for the entire ecosystem to communicate and coordinate, arising out of a single source of truth (data).
3. Real-time feedback loops to enable continual fine-tuning of operations.
4. Increasing transparency of the system, internally and externally.
5. Improvement in delivery of services, reducing leakages and delivering it to the right beneficiaries.

Most government programs today have a clear Information Technology (IT) strategy. Creating an Analytics and Reporting function cannot be done independently of the overall IT strategy of the organization. Hence, while the function can be built independently, Business Intelligence (BI) modules need to be ingrained within the larger IT strategy to be able to function.

Success of this function depends on recognizing that data is the centrepiece, around which the function works. The design should treat data as the platform from which multiple decisions are enabled, rather than just a technology platform that enables access to data. The structure and functioning of the Analytics and Reporting function depends on the objectives and deliverables that the organization expects from it. In most cases, the Analytics and Reporting function acts as a support function to various processes within the organization.

There are 3 broad components to the Analytics and Reporting function – (a) the Business Intelligence (BI) framework that captures and manages data, (b) the Delivery platform through which data is shared within the organization (and potentially outside as well), and (c) the delivery team that enables the function.

BI module has been built within Aadhaar system to provide comprehensive analytics and reports for:

- Partners of UIDAI for effective field management and process improvement via partner portal.
- UIDAI internal users for program monitoring, management, and continuous improvement.

- Public at large via public portal for providing transparency.
- Statisticians and researchers to allow anonymized aggregate data sets for purposes of field studies and advanced research.

UIDAI portals provide a single window for residents, Registrars, Authentication User Agencies (AUAs), and other partners in the ecosystem as well as UIDAI officials to view and manage various types of data generated from the underlying BI system. These self-service portals enable UIDAI to have large ecosystem of partners who can be managed in a systemic process driven way without having to employ large teams of people.

3 Biometric System Strategy

The Aadhaar biometric system design has followed global best practices. UIDAI has reviewed existing state-of-the-art biometric systems, consulted with the world's top biometric experts, conducted a proof of concept study and has built a biometric system that is currently considered state-of-the-art. UIDAI technical experts visited two of the world's largest biometric implementations: US-VISIT program and US Visa/Consular system. UIDAI had meetings with a large number of experts from several countries including Mexico, Bangladesh, UK, the US, Singapore and Australia. Two of the world's most renowned biometrics experts – Prof. Anil Jain and Prof. James Wayman helped the UIDAI team with the strategy and design. Several other biometric experts including Prof. Arun Ross, Prof. John Daugman and Prof. Venu Govindaraju also provided their inputs during design.

UIDAI technical staff visited reviewed and analysed existing biometric programs in India, including the E-shakti, MNREGA in Bihar, Orissa's UNWFR program, AP's Iris based ration card enrolment, Employees State Insurance Scheme (ESIC) and RSBY.

Following this, the Biometric Standards Committee was constituted to study the benchmarks for biometric de-duplication accuracy in other large systems around the world and recommend the approach to be followed by UIDAI to achieve a high de-duplication accuracy to scale to a population of 1.2 billion.

The committee report [6] found that while in the global context, 99% de-duplication accuracy had been achieved using fingerprints alone in a database size of 50 million, 95% de-duplication accuracy could be reasonably expected using 10 fingerprints and face at a database size of 1.2 billion in the Indian context. Hence, the committee recommended that UIDAI explore the use of the iris biometric in

addition to fingerprint and face biometrics to achieve de-duplication accuracy in excess of 99% and also ensure total inclusion.

Based on the recommendation, the UIDAI commissioned a PoC study to determine whether multi-modal de-duplication could improve the de-duplication accuracy. The results of the enrolment PoC showed that an order of magnitude better accuracy could be achieved using a multi-modal de-duplication scheme including both fingerprints and iris.

The PoC report [19] also highlighted the increased inclusiveness of Aadhaar enrolment when iris was added. This is due to the fact that while fingerprint quality was variable among the rural poor due to occupations involving physical labour, the iris does not get worn out with age or use and remained unaffected by most eye surgery. The iris presents a potential means to issue the majority of children a unique number linked to their biometrics, since the iris stabilizes at a very young age.

UIDAI decided to accept the recommendations of the PoC report and capture the following, biometrics for the enrollment of 1.2 billion residents:

- 10 fingerprints
- 2 iris scans
- Photograph of face

The decision [20] to include iris in the Aadhaar initiative was a considered one, and took into account the critical needs of the project in ensuring the uniqueness of the Aadhaar number, and to also ensure that residents, particularly children and the elderly, are not excluded from enrolling for the Aadhaar. The PoC empirically demonstrated that iris is easy to capture, highly accurate, and not too expensive. By guaranteeing the universality and uniqueness of the Aadhaar, the initiative can have a substantial, transformational impact in the lives of residents.

3.1 Enrolment Biometric Quality

The Biometrics Standards Committee recognized that the success of the Aadhaar project depended on the quality of the biometrics captured. The committee recommended the use of ISO standards for the capture of fingerprint, iris, and face biometrics and the usage of lossless compression only, in order to not compromise the quality of the data captured.

3.1.1 Enrolment Biometric Device Certification

A device certification specification for both fingerprint scanner and iris camera was developed in collaboration with STQC in accordance with global standards. UIDAI specified that a standardized VDM (Vendor Device Manager) has to be implemented by each enrolment biometric device to allow for plug and play operation with the Aadhaar enrolment client. As a result, a large number of biometric devices have been able to qualify through certification and compete for business in Aadhaar enrollment ecosystem.

3.1.2 Standardized Enrolment Client

The PoC study helped to create standardized enrolment client software to capture high quality biometrics. Automated checks, both at biometric sensor and software level significantly improved the quality of biometrics captured. The PoC study noted that while the capture of biometrics was more time consuming for older residents, it was well within practical limits.

The standardized client also makes sure that all biometrics captured are distinct (i.e. there are no repetitions of biometrics) and the biometrics of the operator are not inadvertently included in the resident packet. By continuously measuring the quality of the biometrics using BI system, and providing feedback for improving the process for collecting biometric data, the system is designed to make sure that the quality of collected biometric data stays high and does not degrade. When enrollment agencies receive feedback on the quality of their enrolments, it leads to improvements in their training and processes, since their payments are linked to successful Aadhaar numbers generated and not number of enrolments conducted.

The biometric accuracy report [19] about the quality of Aadhaar data based upon the study of 84 million enrolments shows that only 2.9% of residents have poor quality fingerprints, and only 0.23% residents have both poor quality fingerprint and poor quality iris captures as a result of the measures taken to ensure the quality of biometric data capture.

3.2 Multi-ABIS Backend System

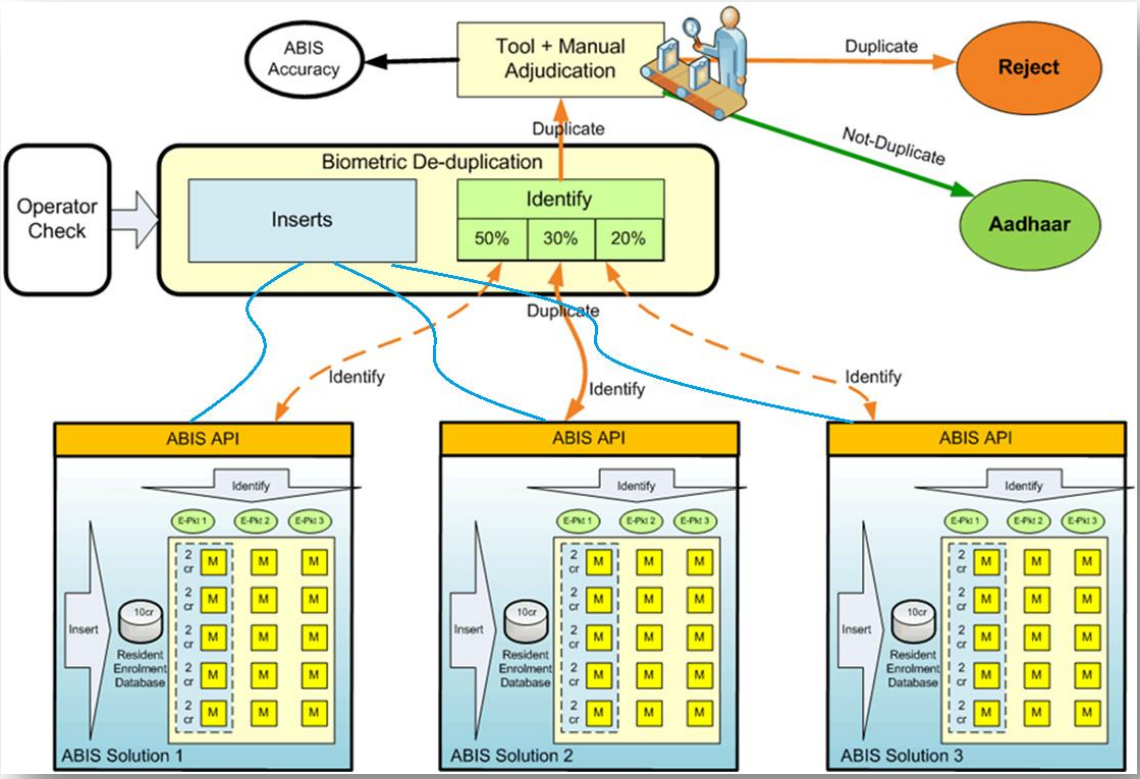
Since de-duplication at this scale (1.2 billion residents) had not been previously attempted anywhere in the world, UIDAI decided to procure 3 ABIS (Automatic Biometric Identification System) software solution to perform biometric de-duplication as a risk mitigation strategy.

Aadhaar is the first ever multi-ABIS system implemented in the world, and brings significant advantages:

- It ensures that there is no vendor lock-in. If one of the ABIS solutions needs to be replaced (for any reason - technical or contractual), it can be done without bringing the entire system to a grinding halt.
- The three ABISs compete for work based on their accuracy and throughput. Since payment is based on successful de-duplication (not an upfront payment for software), solution providers compete to improve accuracy and throughput aiming for a higher volume of de-duplications.
- The deployment of multiple ABISs improves the accuracy of de-duplication. If any ABIS identifies a potential duplicate, it is sent to the other ABIS for verification. By combining the results of all 3 ABIS systems the overall biometric de-duplication accuracy goes up.
- The utilization of three different de-duplication engines with different implementations and fusion strategies also helps to detect various kinds of software or data collection errors. In certain enrolments (for example in suspected duplicates and enrolments with poor quality biometrics) the enrollment data is sent to more than one ABIS to minimize the chance of an identification error.

- The use of multiple ABIS engines also permits continuous monitoring. Each duplicate found is used as a "probe" to test the accuracy of the other two ABIS systems. This is critical to maintain the accuracy of the system on an ongoing basis.

Following diagram depicts logical flow of de-duplication requests.



3.3 Biometric Accuracy

The enrolment accuracy study [19] conducted with a gallery size of 84 million, provided definitive evidence that Aadhaar enrolment can exceed its accuracy goals.

The False Positive Identification Rate (FPIR) was measured to be 0.057%. In practical terms, it means that at a run rate of 10 lakh enrolments a day, only about 570 cases need to be manually reviewed daily to ensure that no resident is erroneously denied an Aadhaar number. The UIDAI currently has a manual adjudication team that reviews and resolves these cases.

The False Negative Identification Rate (FNIR) was measured to be 0.035%. This implies that 99.965% of all duplicates submitted to the biometric de-duplication system are correctly caught by the system as duplicates. Given that currently approximately 0.5% of enrolments are duplicate submissions, only a few thousand duplicate Aadhaars may possibly be issued when the entire country of 120 crores is enrolled.

Based on the analysis, it can be stated with confidence that Aadhaar enrolment system has proven to be reliable, accurate and scalable to meet the nation's need of providing unique Aadhaar numbers to the entire population. It is now safe to conclude that the system will be able to scale to handle the entire population.

3.4 Fingerprint Authentication PoC

The UIDAI published a report on the findings of a series of Proof of Concept (PoC) studies carried out by UIDAI from Jan 2011 to Jan 2012 on Aadhaar biometric authentication [18]. The PoC studies focused on fingerprint biometric and its impact on authentication accuracy in the Indian context. The key findings of the report are:

- Determining the 'best finger' of residents so that they can use their best fingers for authentication improves the authentication accuracy.
- Using the resident's best finger, single-attempt gives an accuracy of 93.5%.
- Using multiple (up to 3) attempts of the same best finger improves the accuracy to 96.5%.

As a result of this, UIDAI has mandated that all Aadhaar authentication application providers should provide Best Finger Detection (BFD) application to improve authentication outcomes when required. Using 2 best fingers improves the accuracy further since more information is available to perform the matching. All Aadhaar authentication applications first attempt single finger authentication, followed by multiple attempts of two finger authentication if necessary to obtain the highest level of accuracy.

There were differences in performance of different sensor-extractor combinations. This was observed under general conditions as well as across age groups. One of the unique aspects of the authentication device certification was requirements to meet Aadhaar accuracy goals in a field test. The first Performance Testing of Biometric Devices (Finger print Scanner) for authentication purpose was conducted) from 15th July, 2012 to 24th July, 2012 at Mayur Vihar Phase II, Delhi. During the testing, 36 combinations of various products were tested on a live authentication set up using the same human test population of more than 5000 residents (having Aadhaar numbers).

3.5 Iris Authentication PoC

Two Proof of Concept (PoC) studies were carried out for iris-based authentication. The first PoC study showed that iris authentication can be used to authenticate over 99% of the residents [20]. Operating at false accept rate of one in million, iris technology also lends itself for highly secure authentication against imposter attacks. The PoC also showed that six different devices with a variety of form and function are available to form competitive vendor eco-system. The second PoC study showed that the iris authentication accuracy was not significantly impacted by KIND7 compression, which resulted in an average image size of 2-3KB. The PoCs enabled identification of device specifications and certification procedure necessary for iris authentication devices.

4 Aadhaar e-KYC

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

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a key requirement for access to financial products (payment products, bank accounts, insurance products, market products, etc.), SIM cards for mobile telephony, and access to various Central, State, and Local Government services. Today, customers provide physical PoI and PoA documents. Aadhaar is already a valid PoI and PoA document for various services in the Financial, Telecom, and Government domains.

The Aadhaar e-KYC API [14] provides a convenient mechanism for agencies to offer an electronic, paper-less KYC experience to Aadhaar holders. The e-KYC service provides simplicity to the resident, while providing cost-savings from processing paper documents and eliminating the risk of forged documents to the service agencies. UIDAI has published its policy on e-KYC [5] and e-KYC API is implemented as per the policy.

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

4.1 Salient Features of the e-KYC Service

1. **Paperless** – The service is fully electronic, and physical document management can be eliminated.
2. **Consent based** – The KYC data can only be provided upon authorization by the resident through Aadhaar authentication, thus protecting resident privacy.
3. **Eliminates document forgery** – Elimination of photocopies of various documents that are currently stored in premises of various stakeholders reduces the risk of identity fraud and protects resident identity. In addition, since the e-KYC data is provided directly by UIDAI, there is no risk of forged documents.
4. **Inclusive** – The fully paperless, electronic, low-cost aspects of e-KYC make it more inclusive, enabling financial inclusion.
5. **Secure and compliant with the IT Act** – Both end-points of the data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper documents. In addition, the use of encryption and digital signature ensures that no unauthorized parties in the middle can tamper or steal the data.
6. **Non-repudiable** – The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital signature by UIDAI when providing the e-KYC data makes the entire transaction non-repudiable by all parties involved.
7. **Low cost** – Elimination of paper verification, movement, and storage reduces the cost of KYC to a fraction of what it is today.
8. **Instantaneous** – The service is fully automated, and KYC data is furnished in real-time, without any manual intervention.
9. **Machine readable** – Digitally signed electronic KYC data provided by UIDAI is machine readable, making it possible for the service provider to directly store it as the customer record in their database for purposes of

service, audit, etc. without human intervention making the process low cost and error free.

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

4.2 Compliance with the IT Act, 2000

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

1. The e-KYC electronic record provided by the UIDAI is equivalent to the Aadhaar letter (Section 4 of the IT Act, 2000);
2. A cryptographic hash of the KYC data is computed and attached. The SHA-2 digital hash function algorithm is used. Hashing ensures that any tampering of the data in transit is detected (Section 3 of the IT Act, 2000);
3. The KYC data along with the computed hash are encrypted using a combination of AES-256 symmetric key and RSA-2048 PKI encryption, form a secure electronic record. The encryption ensures that only the intended service provider can view the data provided by the UIDAI (Section 14 of the IT Act, 2000); and
4. The encrypted data and hash are digitally signed by the UIDAI using RSA-2048 PKI. The secure digital signature of UIDAI can be verified by the service provider to ensure the authenticity of the source (Section 15 of the IT Act, 2000).

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

5 Data Privacy & Security

Security and privacy of personal data has been fundamental in design of Aadhaar system without sacrificing utility of the national identity system. When creating a national identity system that stores and manages data about a billion people, it is imperative that privacy and security of personal data become a key discussion point.

5.1 Privacy by Design

Security and privacy of personal data has been fundamental in design of Aadhaar system without sacrificing utility of the national identity system. When creating a national identity system of this scale, it is imperative that privacy and security of personal data are not afterthoughts, but designed into the strategy of the system from day one.

Aadhaar system addresses these issues at its core. Following key aspects are results of this.

5.1.1 Aadhaar Numbering Scheme

Aadhaar number is a random number with no built-in intelligence or profiling information. A 12-digit number was chosen based on the identification needs of the population in the next couple of centuries [21].

It was also decided that, to ensure privacy, the date-of-birth and other attribute information should not be embedded in the number. Similarly, place of birth or

residence using administrative boundaries (state/district/taluk) should also not be embedded within the number. When state/district IDs are embedded, the number faces the risk of becoming invalid and misleading the authenticator when people move from place to place. It can also lead to profiling/targeting based on the region/state/district that a person is from. The approach of storing intelligence in identification numbers was developed to make filing, manual search and book-keeping easier prior to the advent of computers. This is no longer necessary, since centralized database management systems can index the records for rapid search and access without having to section data by location or date of birth.

5.1.2 Minimal Data with No Linkage

Since Aadhaar system has data of all Aadhaar holders of the country in a central repository, it was essential that data be kept to a minimum so as to provide identity related functions (issuance and authentication) and nothing else. This design philosophy is derived directly from the fact that UIDAI respects privacy of the residents and not hold non-essential data within its systems.

In addition to having minimal data (4 attributes – name, address, gender, and date of birth - plus 2 optional data – mobile, email), this central database does not have any linkage to existing systems/applications that use Aadhaar.

This essentially creates a set of data islands containing resident data across various applications/systems (a federated model for resident data) rather than a centralized model eliminating the risk of a single system having complete knowledge of resident and his/her transaction history.

5.1.3 No Pooling of Data

Aadhaar system is not designed to collate and pool various data and hence does not become a single central data repository having all knowledge about residents. It has no linkage information (such as PAN number, Driver's License Number, PDS card number, EPIC number, etc) to any other system. This design allows transaction data to reside in specific systems in a federated model. This approach allows resident information to stay in distributed fashion across many systems

owned by different agencies. Any transfer or collation of data across these distributed information silos should follow due course of law.

5.1.4 Yes/No Answer for Authentication

Aadhaar authentication responds only with yes/no answer. For example, authentication answers questions such as "*resident claims his/her name is ..., is this correct?*" whereas it does not provide any scheme to ask questions such as "*what is the address of resident whose Aadhaar number is ...?*". Aadhaar authentication allows applications to "verify" the identity claim by the resident while servicing them while still protecting their data privacy.

5.1.5 Explicit Resident Consented e-KYC

A balance between 'privacy and purpose' is critical to ensure convenience of online identity is balanced with the requirement to protect resident identity data. External user agencies do not have access to the Aadhaar database. Aadhaar e-KYC service allows resident to authorize UIDAI to share electronic version of their Aadhaar letter. For every Aadhaar e-KYC request, only after successful resident authentication, demographic and photo data is shared in electronic format (via biometric/OTP authentication resident explicitly authorizes UIDAI to share electronic version of Aadhaar letter instead of sharing physical photocopies). Resident authorization is NOT used for multiple e-KYC transactions, instead, every time agencies require electronic version of Aadhaar letter data for KYC purposes, resident must authorize the agency.

5.1.6 No Transaction History

Aadhaar authentication does not have any knowledge of the transaction resident is performing. It only knows that resident is authenticated by this agency at this time. Aadhaar system has no knowledge and is not designed to keep track of specific transaction details such as depositing money or obtaining pension or anything else. This has been consciously designed to ensure resident transaction history is not part of a central system to ensure privacy of the resident.

5.2 Resident Data Security

It is critical to ensure security of resident data including biometrics. Aadhaar system has implemented various techniques across the system to ensure data confidentiality and integrity.

5.2.1 Enrolment Data Security

The enrolment/update data packets are encrypted by the client using public key cryptography with each data record having an HMAC which can identify any integrity violation of the data. Master keys are stored and managed within HSM (Hardware Security Module) appliance.

Following should be noted:

- Every enrolment station, registrar, enrolment agency, operator, and supervisor are registered and authenticated.
- Every packet is biometrically signed by operator (and supervisor in various cases) and contains complete process data including station ID, timestamp, location (pin code, GPS). This allows strong validations and traceability at packet level.
- Every enrolment data packet is "always" stored in encrypted, tamper-evident files and are never decrypted or accessed during transit.
- Enrolment data is "never" decrypted until it is reached within UIDAI's data centre's secure production zone.

Usage of strong 2048-bit PKI encryption technologies ensures that no agencies or persons can access, modify, or misuse the resident data during field enrolment or in transit to the UIDAI data centres.

In addition to enrolment packet, resident data in Aadhaar master database and BI data store is protected through various security measures. These include:

- **Encryption** – Ensures data is encrypted and not available to administrators and other users in plain text format.
- **Anti-Tampering** – Ensures data is only altered by authorized applications and not via command line SQL scripts.
- **Data Partitioning** - Data is partitioned and stored across multiple databases with a random alias being the only link to ensure there is no central database table where all resident data is available.
- **Anonymization** – Hashing techniques are used for anonymizing data in BI/Reporting data store, and yet retaining the ability to do analytics.

Other than application techniques as described above to protect resident data, UIDAI has implemented data centre best practices and technologies such as firewalls, IPS systems, zoning and access control, centralized security policy management, audits, 24x7 monitoring through Security Operations Centre (SoC), and strong security procedures used to ensure CIDR is protected.

5.2.2 Authentication & e-KYC Data Security

Aadhaar authentication and e-KYC services use open security standards to secure data and service end-points and are designed to address transaction privacy.

Both Authentication and OTP API detail mechanisms to secure the data in transit by proposing usage of encryptions, HMAC, and digital signatures, and ensure that data cannot be stolen or modified in transit, and its authenticity and origin can also be verified. API data is encrypted with a dynamic session key using AES-256 symmetric algorithm (AES/ECB/PKCS7Padding). Session key, in turn, is encrypted with 2048-bit UIDAI public key.

Aadhaar authentication records all the authentication requests and their responses for audit purposes. Notification inbox containing last "*n*" months of notifications is maintained for each resident and available for resident's viewing, where value of "*n*" is determined by the audit retention policy of the UIDAI. All authentication and e-KYC responses are digitally signed by UIDAI which helps AUAs to maintain

electronic audits. Audit trail stores the request and response XMLs along with unique response code as the audit key.

Within the UIDAI backend systems, Aadhaar Number is not stored in any of the authentication database. Instead, a SHA-1 hash of Aadhaar Number is stored. In addition, record level encryption and tamper detection features ensure resident data within authentication data store is neither available to any internal user nor can it be modified by unauthorized users or applications.

When publishing events to BI system for analytics, an internal alias is published instead of Aadhaar number, and entire BI system is stripped off all PII data.

Since many applications and services across the country may heavily depend on Aadhaar authentication, it is strategically important not to expose Aadhaar authentication over Internet (or any public network) and create a "single point" of attack that can potentially affect many services. Creation of ASA as a network service provider and exposing authentication service only through secure private connections is strategic to ensure multiple end points always exist to provide authentication service in a secure and always available fashion. As per UIDAI policy, authentication and other online services such as e-KYC are never exposed over Internet or any public network [22].

In the case of e-KYC, for every Aadhaar e-KYC request, only after successful resident authentication, demographic data and photo are shared in electronic format (via biometric/OTP authentication resident explicitly authorizes UIDAI to share electronic version of Aadhaar letter instead of sharing physical photocopies). Resident authorization is NOT used for multiple e-KYC transactions, instead, every time agencies require electronic version of Aadhaar letter data for KYC purposes, resident must authorize the agency.

6 Financial Inclusion

Aadhaar can play an important role in driving financial inclusion, by simplifying key processes in account opening and electronic payments:

- Aadhaar e-KYC for Know Your Customer (KYC) requirements;
- Aadhaar number as a financial address for receiving and sending funds; and
- Aadhaar authentication for authorizing electronic transactions.

6.1 Achieving Inclusion using Aadhaar KYC

Once an Aadhaar number is issued to a resident, the resident's demographic and biometric data can be electronically authenticated. For every authentication request received by UIDAI, the Authority will return an encrypted and digitally signed response (as per the provisions of the IT Act, 2000).

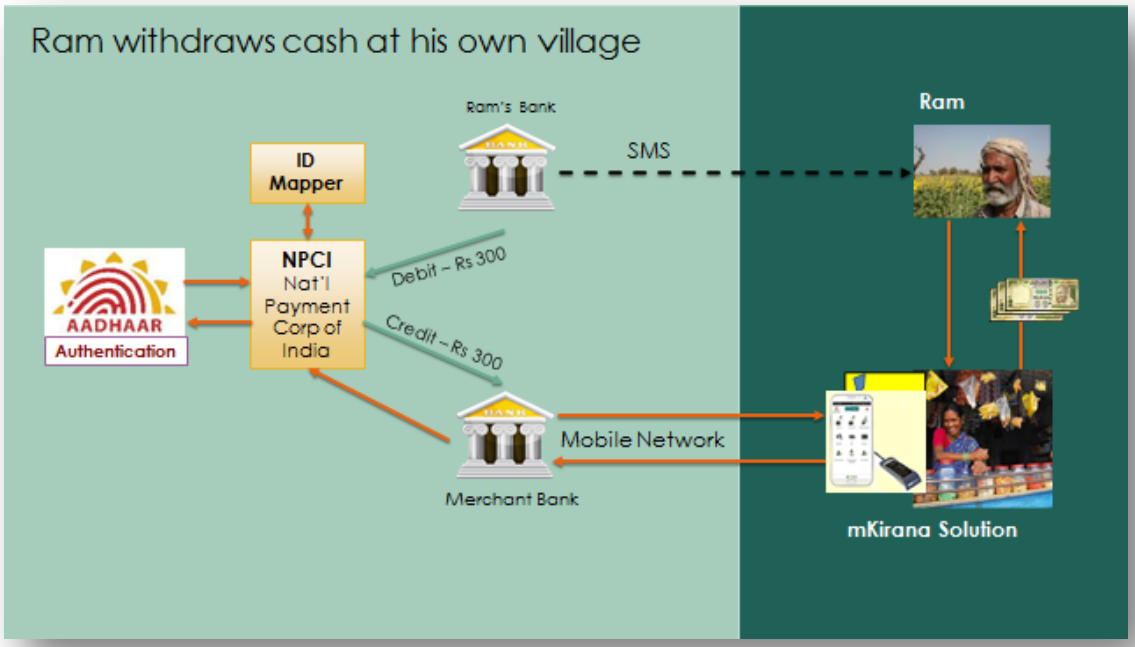
The following progress has been made in acceptance of Aadhaar as KYC for financial products:

1. The Ministry of Finance has amended Rule 2(1)(d) of the Prevention of Money Laundering Act, 2005, adding Aadhaar to the list of officially valid documents[1].
2. The Reserve Bank of India (RBI) has also issued a notification to banks along the same lines by including Aadhaar as a valid PoI and PoA document for opening bank accounts with full KYC[2].
3. The Insurance Regulatory and Development Authority (IRDA) has notified Aadhaar as a valid KYC document to insurance companies[3].

[1] http://uidai.gov.in/images/FrontPageUpdates/notification_regarding_aadhaar.pdf

[2] http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=6739&Mode=0

4. The Securities and Exchanges Board of India (SEBI) has notified Aadhaar as a valid KYC document[4].
5. The Department of Telecommunications has notified the Aadhaar document and electronic Aadhaar authentication for PoI and PoA in order to activate a telecom connection[5].



This facility of online authentication offered by the UIDAI is important in the context of electronic delivery of services:

1. The Information Technology Act, 2008 provides for parity between physical and electronic documents;
2. The Report of the Inter-Ministerial Group on a Framework for Delivery of Banking Services via Mobiles proposes a payments solution based on mobile and Aadhaar number linked accounts.
3. The Electronic Services Delivery Bill paves the way for electronic provision of services;

---

[3] http://uidai.gov.in/images/FrontPageUpdates/kyc_for_insurance_sector.pdf

[4] http://www.sebi.gov.in/cms/sebi_data/attachdocs/1317809779732.pdf

[5] http://www.dot.gov.in/as/2011/as_14.01.2011.pdf

4. The draft Mobile Governance Framework put forward by DIT strives to set up a framework for rolling out mobile based delivery of public services; and
5. A draft of a triad of policies to drive a national agenda for ICTE (Information and Communications Technology and Electronics) defined by DIT.

6.2 Aadhaar as a Financial Address

The advent of e-mail has ensured that the concept of a physical address and the physical location of individuals and institutions have gradually become redundant for communication. Similarly, the ability of the Aadhaar number to uniquely identify an individual electronically makes it a valuable tool in the administration of Government schemes, and a natural financial address on the basis of which funds can be transferred into a linked account. The beneficiaries may link their Aadhaar number to their account at any bank, and change this at any time, based on the quality of service they receive. Aadhaar as a financial address makes the bank account portable for the purpose of receiving Aadhaar-addressed payments.

Permanency of Aadhaar provides a great mechanism to continue sending money even after several years since initial seeding. While the Aadhaar holder gets the benefit of moving from one bank to another without having to inform all agencies, applications sending money can continue working, making overall information maintenance cost very low.

6.2.1 Benefits for Government

The Government benefits in the following ways by using Aadhaar as a financial address:

1. Seeding the Aadhaar number in a scheme's database helps remove ghost, duplicate, and fake identities, making it possible for scarce development funds to be used in an effective manner;
2. Aadhaar can provide various government departments with a platform approach for all EBTs and subsidy payments leading to standardized procedures and reporting platform; and

3. Government can make payments only on the basis of Aadhaar numbers, without focusing on collecting bank account details, and focusing on service delivery.

6.2.2 Benefits for Customers

Customers benefit in the following ways by using Aadhaar as a financial address:

1. The customer's Aadhaar-enabled account can be used for receiving multiple welfare payments as opposed to the one-scheme, one-bank approach followed by a number of State Governments/Departments;
2. The Aadhaar number serves as a robust and stable financial address for sending and receiving remittances; and
3. Aadhaar authentication can ensure that the funds are used by the intended beneficiary thereby reducing chances of rent-seeking by middlemen.

6.2.3 Benefits for Policy Makers

Policy makers benefit in the following ways by using Aadhaar as a financial address:

1. Sending Government payments to Aadhaar-linked accounts will lead to those accounts becoming active and achieve greater financial inclusion; and
2. Aadhaar linked fund flows from the Government to the customer gives full traceability, audit, and non-repudiation.

6.3 Aadhaar Authentication for Transactions

The purpose of Aadhaar authentication is to enable residents to prove their identity and for service providers to confirm that the residents are *who they say they are* in order to provide services and access to benefits. Aadhaar authentication can be used to verify the identity of residents in the case of financial transactions using micro-ATMs. The RBI Working Group on Card Present Transactions has also recommended the use of Aadhaar authentication as an additional factor[6].

[6] http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/SCP020611FS.pdf

Biometric authentication has become socially acceptable, proven to work at scale, and addresses the challenges of remembering PINs, passwords and operating equipment such as mobile phones, ATMs, etc. In general, payment system operators may use any secure and approved method for authentication of customer's identity. However, for certain vulnerable sections of society, where Government payments are being disbursed, the Government may mandate Aadhaar-based biometric authentication. In some cases, the Government may also want to ensure that the payments are made to the woman of the household so they are utilised in an appropriate manner.

Since Aadhaar may be used as KYC for a number of services, it is essential that the Aadhaar-linked data is current and correct. In order to achieve this, the UIDAI is setting up update centres throughout the country with the help of registrars. This network of Aadhaar update centres, combined with other locations such as Post Offices, Citizen Service Centres, etc. provide an infrastructure that can be leveraged by financial institutions for lifecycle management of customer data and PIN/password management. For example, in cases when someone forgets or loses their PIN/password, or wishes to update their mobile number, they can do so at such a centre in person, using biometric authentication.

6.4 APBS, AEPS, and IMPS Systems of NPCI

National Payment Corporation of India (NPCI) offers 3 systems to make Aadhaar enabled financial system possible. They are:

1. **Aadhaar Payment Bridge System (APBS)**: Provides an easy to use mechanism for electronic credit such as government subsidy payments, salaries, etc. on the basis of Aadhaar numbers as the unique identifier and global address and an end-to-end visibility for such transactions. In the case of government subsidy payments, it ensures no duplicates/fakes exist in the system thereby reducing leakages.
2. **Aadhaar Enabled Payments System (AEPS)**: It is a payment mechanism that uses online Aadhaar authentication for customer identification. The online, inter-operable architecture of AEPS allows a resident to access his/her account from anywhere in the country and across any delivery

channels such as ATMs, micro-ATMs, etc. The interoperable architecture of AEPS and micro-ATMs enables online and real-time fund transfer across banks thus enabling an efficient and cost-effective remittance ecosystem.

3. **Immediate Payment Service (IMPS)**: It offers an instant, 24X7, interbank electronic fund transfer service through mobile phones. IMPS facilitate customers to use mobile instruments as a channel for accessing their bank accounts and put high interbank fund transfers in a secured manner with immediate confirmation features. This system is now being enhanced to support payment to Aadhaar number. This allows person-to-person payments using just Aadhaar numbers as the source and destination addresses.

Most banks in India are part of NPCI network taking advantage of above systems and are starting to allow usage of Aadhaar in various payment transactions across their banking systems.

7 Mega Technology Trends

Let us look at the challenges of creating systems of public good, and how the UIDAI has attempted to address these challenges through effective digital governance. We will also look at the mega trends that have made such an identity system possible.

The challenges of creating public good in India are immense. Public good must be universal so that everyone can have access to it; ubiquitous, so that access is available anywhere; inclusive, so there is no bias against those who need it most; uniform, so basic national goals are met and yet, must address diverse requirements of every region and community which differ in their geography, language and customs.

Public good creation and delivery must reflect the federal structure of Centre, States and urban/rural local bodies. It is important to recognize that there are many providers of public services who are often in silos, often at odds with each other in the timing, mode and nature of the service to be provided. This leads to very high coordination costs, even if such coordination were technically feasible. Expertise is scarce and is usually urban-centric. Solutions must be scalable to over a billion people and be implemented with speed in the face of rising expectations, and with the demographic dividend being time bound.

This complexity has often been the reason that the promise of 'e-governance' has not been fully or uniformly realized. The scepticism engendered has led policy makers to fall back on the same old methods of 'reform', including passing laws, defining rights and creating new oversight bodies, which often address the symptoms but not the disease, and make governance even more dysfunctional.

7.1 Mega Trends Making 'Digital Governance' Effective

The last decade has seen some tectonic shifts in the IT and communication technology that make digital governance a powerful and inclusive solution today. These trends offer India a radically different way to reform public service delivery.

1. **Consumerization and Gamification**: A few years ago, the centre of gravity in technology innovation was the enterprise. In the last 3-4 years it has moved to the consumer (iPad, Android, etc) and to Games (Kinect, Wii, MMOGs). Hence greater computing power and better graphics have evolved, keeping in mind ease of use for the consumer. The cloud has also helped in absorbing complexity. This in turn means that we can design resident-facing applications that are very simple and easy to use for people who may have been challenged by traditionally complex technology.

2. **Better Hardware**: Today's devices can be smaller, lighter, thinner, with long battery life, and large screens. This makes them ideally suited for crowded offices, schools, health centres and grocery stores. They can be charged in the morning and used all day. They do not need air-conditioning, have no moving parts and make no noise. They can switch between Wi-Fi and the cellular network based on availability.

3. **End of the Keyboard**: The end-user devices today have video, touch interfaces (familiar to any voter who has used an EVM), biometric recognition, voice interfaces coupled with apps like Siri and motion sensors like Kinect. All of these have great implications in bridging the 'literacy' divide as the keyboard becomes obsolete, at least for content consumption.

4. **Low cost**: Today's market dynamics shaped by huge volumes, commodity chips and software, and fab-less chip design rapidly drive down the cost of devices. This is further accentuated because the new revenue models do not need to envisage margins from selling hardware and software. This puts

high quality devices at low cost in the hands of millions. Tomorrow's broadband Telcos could bundle a low-cost tablet with 4G/LTE.

5. **Real-time feedback**: The re-engineering of public service delivery can ensure that data is captured at the point of service delivery, i.e. on the device as delivery happens. This can be highly granular. Once the information is on the cloud you can build a near real-time system which gives results, effect of policies, performance measurement, fraud, audit and other management inputs, with the use of techniques such as "Big Data' GIS, GPS, visualization tools, etc. This can take policy decisions away from ideological battles ('cash transfers don't work because the beneficiary will drink it away') to more fact-based policy making and a continuous improvement approach. Instant high quality feedback will give administrators and funders a good reason to buy into this approach.

6. **Hub and Spoke**: The cloud allows people with expertise like specialist doctors, teachers and nutritionists to spread their expertise and skills over a large number of recipients. Similarly, high quality content can be a created by a few, like the Khan Academy, and when coupled with automated language translation can be made available to a vast audience.

7. **Participative Systems**: Initiatives like data.gov and API-based design will allow people to analyse and mash up data and services for new applications. Social Networking will enable volunteers to be brought into public service delivery. Communities and beneficiaries can give feedback over the Web, IVRS or through text messages.

8. **Empowering front-line workers**: Today's workers in the field, the ASHAs, ANMs, Anganwadi workers, para-teachers, who number close to 2 million, spend a large portion of their time filling out registers and reports. Significant amount of time is also spent in collecting their stipend and incentives. With data capture happening at the point of service delivery and payments being streamlined, front-line workers will have more time and

motivation to serve people. With sensor 'swarms', data like ECG, BP, height and weight can directly be captured and sent to the cloud which again will improve the worker's productivity and of course contribute to much better data quality.

9. **Inclusive applications**: The normal process for 'eligibility' in any public service includes high entry barriers leading to discretion, corruption and exclusion and no exit, as the backend systems do not exist. With strong applications and data analytics, this can be reversed by making the entry welcoming, even based on self-declaration and using the backend to identify fraud and ensure punishment. The end-to-end ability to audit and non-repudiation that Aadhaar-based authentication provides will help in developing such systems.

10. **Stitching together**: NIUs (like PDSN and GSTN), services offered on the cloud, and the mobile/tablet as the delivery device for both self-service and assisted service, enable an asynchronous development and deployment model where each app can be launched at its own pace. As long as each public service delivery agency follows a few simple rules, the application will be interoperable with the rest. This hugely reduces coordination costs which are often the biggest challenge.

7.2 Technology-enabled Governance Transformation

Aadhaar has used technology extensively to bring about governance transformation at scale. There are various advantages in adopting technology to achieve improved governance. The key drivers are:

1. **Scale**: Any social problem that needs to be fixed in India involves millions of people and billions of transactions. This is true of food distribution, health care and educational outcomes. IT based solutions, specifically the Internet class systems of today, offer a way to meaningfully address this.

2. **Speed**: India is sitting on a demographic bulge of young people with high aspirations and expectations. Hence solutions will have to be capable of being rolled out in months and years, not in decades. The technology world, due to Moore's law, rapid innovation, extreme competition, network effect, ecosystems and rapid learning through quick feedback loops and data analytics, has shown how this can be done.

3. **Cost**: Any solution has to be cost-effective to be meaningful. Again, the tech world has shown how cost can be reduced through factors like innovation and repeatability.

4. **Enforceability**: The ability to ensure that things are done only in a particular way is very important. This helps in quality, auditability transparency, safety and in maintaining performance standards and service levels. This is inherent in a technology solution.

5. **Diversity**: While some standard operating procedures need to be enforced, a good design will allow for adaptable and diverse solutions to be built. The 'platform' approach allows such 'apps' to be developed, unleashing innovation and creating custom solutions to diverse problems. Aadhaar is an example of a platform built using innovation and used for further innovation.

6. **Autonomy**: The federal governance structure of India requires platforms that are able to combine scale and standards with enough autonomy for each agency. For e.g., GST uses common tax payer ID and invoice matching to reduce evasion and increase revenue, but allows each state to have its own audit and investigative procedures.

7. **Mobility**: Given that we are going to see rapid mobility due to demographic differences, employment opportunities, etc. any solution has to be

accessible everywhere in the country with the same service level. This is only possible with a solution in the cloud.

8. **Inclusion**: Technology allows inclusion by lowering cost, enabling smaller transaction sizes ('the sachet' approach), going digital/paperless, allowing geographic accessibility and choice through portable benefits. It enables a model where access is universal and the defaulters are caught through technology as opposed to one where honest people are greatly inconvenienced in order to catch a few wrongdoers. The 'hub and spoke' allows scarce expertise to be made available to everyone, even if the final service provider is not highly skilled.

9. **Best of breed components**: Using data as an integrator, entire solutions can be 'snapped' together' with best of breed components from public, private and NGO sector. The Aadhaar enrolment system is an example.

10. **Collaboration**: The availability of public services as a platform, like an Identity platform, payment platform, GIS platform and GST platform, forces collaboration. It also allows every state, region or participant to get access to the same level of domain knowledge which gets continually enhanced. For e.g., the GST platform gives the same capability to both advanced and weak states. An auction platform brings state of the art auction techniques to maximize government revenues in all natural resource auctions.

8 Conclusion

Aadhaar system is built on a sound strategy and a strong technology backbone which enabled the program to be launched ahead of plan in Sept 2010 and reach the kind of scale that was never achieved in any biometric identity systems across the world. Aadhaar has created an ecosystem of partners for various key components of the project and integrated all these partners using a technology backbone. Aadhaar system defined standards and application programmatic interfaces (APIs) to ensure openness, vendor-neutrality, security and scale. This approach led to a tightly integrated system that could generate 600million Aadhaars in 4 years.

A benefit of Aadhaar integration into the financial system of the national payment switch (NPCI) and integration with Bank KYC ensured 'financial inclusion' for large numbers of people. The AEPS (Aadhaar Enabled Payment System) and APB (Aadhaar Payment Bridge) were key components of financial inclusion that came out of the Aadhaar project. In the absence of digital privacy laws, Aadhaar took it upon itself to implement rigorous standards and measures to ensure data privacy and security of the system. Both the enrolment and authentication systems were designed to protect and safeguard data privacy of the resident.

Certain key mega trends in technology helped Aadhaar build and implement one of the most ambitious e-Governance projects in the world. Within a short span of 4 years since launch, Aadhaar system delivered more than 600 million Aadhaar numbers and is poised to transform the services delivery infrastructure of the country.

References

[1] UIDAI, "UIDAI Strategy Overview," http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf, 2011.

[2] UIDAI, "UIDAI Background," http://uidai.gov.in/all-about-uidai/uidai-background.html, 2009.

[3] UIDAI, "Aadhaar Authentication Framework," http://uidai.gov.in/images/authDoc/d2_authentication_framework_v1.pdf, 2012.

[4] UIDAI, "Aadhaar Authentication Operating Model," http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf, 2012.

[5] UIDAI, "Aadhaar E-KYC Service - Policy," http://uidai.gov.in/images/ekyc_policy_note_18122012.pdf, 2012.

[6] UIDAI, "The Biometrics Standards Committee Report," http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf, 2010.

[7] UIDAI, "Aadhaar Product Document," http://uidai.gov.in/images/AadhaarProductDoc_mar2014.pdf, 2014.

[8] UIDAI, "Aadhaar Technology Architecture," http://uidai.gov.in/images/AadhaarTechnologyArchitecture_mar2014.pdf, 2014.

[9] UIDAI, "The Demographic Data Standards and verification procedure Committee Report," http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf, 2009.

[10] UIDAI, "Aadhaar Automated Biometric Identification System (ABIS) API," http://uidai.gov.in/UID_PDF/Working_Papers/Aadhaar_ABIS_API.pdf, 2010.

[11] UIDAI, "Aadhaar Biometric SDK API Version 2," http://uidai.gov.in/images/aadhaar_biometric_sdk_api_2_0.pdf, 2012.

[12] UIDAI, "Aadhaar Biometric Capture Device API," http://uidai.gov.in/UID_PDF/Working_Papers/UID_Biometrics_Capture_API_draft.pdf, 2010.

[13] UIDAI, "Aadhaar Authentication API 1.6," http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf, 2012.

[14] UIDAI, "Aadhaar E-KYC API 1.0," http://uidai.gov.in/images/aadhaar_kyc_api_1_0_170912.pdf, 2012.

[15] UIDAI, "Aadhaar Best Finger Detection (BFD) API 1.6," http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf, 2012.

[16] UIDAI, "Aadhaar One-Time-Request (OTP) API 1.5," http://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf, 2012.

[17] UIDAI, "Role of Biometric Technology in Aadhaar Authentication," http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf, 2012.

[18] UIDAI, "Role of Biometric technology in Aadhaar Authentication," http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf, 2012.

[19] UIDAI, "Role of Biometric Technology in Aadhaar," http://uidai.gov.in/images/FrontPageUpdates/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf, 2012.

[20] UIDAI, "Iris Authentication Accuracy - PoC Report," http://uidai.gov.in/images/iris_poc_report_14092012.pdf, 2013.

[21] UIDAI, "UID Numbering Scheme," http://uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf, 2010.

[22] UIDAI, "Aadhaar Authentication Security Model," http://uidai.gov.in/images/authDoc/d3_4_security_policy_framework_v1.pdf, 2012.

[23] UIDAI, "Analytics : Empowering operations - The UIDAI Experience," http://uidai.gov.in/images/FrontPageUpdates/uid_doc_30012012.pdf, 2012.

[24] UIDAI, "Aadhaar Enabled Service Delivery," http://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf, 2012.

[25] Data.Gov, "Data Portal for Government of India," http://data.gov.in/, 2012.

[26] UIDAI, "UIDAI Data Update Policy ver 2.1," http://uidai.gov.in/images/update_policy_version_2_1.zip, 2012.

[27] Wikipedia, "Universally Unique Identifier," http://en.wikipedia.org/wiki/Universally_unique_identifier, 2012-2013.

[28] Oracle, "Java 6 UUID Class," http://docs.oracle.com/javase/6/docs/api/java/util/UUID.html, 2011-2013.

[29] W3C, "Extensible Markup Language (XML)," http://www.w3.org/XML/, 2012.

[30] Google, "Protocol Buffers," https://code.google.com/p/protobuf/, 2013.

[31] STQC, "Bio-metric Devices Testing and Certification," http://stqc.gov.in/content/bio-metric-devices-testing-and-certification, 2011-2013.

[32] UIDAI, "Aadhaar Web Portal," https://portal.uidai.gov.in/, 2009-2014.

[33] UIDAI, "Aadhaar Registered Devices Specification," http://uidai.gov.in/images/aadhaar_registered_devices_1_0.pdf, 2014.

[34] UIDAI, "Aadhaar One-Time-Request (OTP) API 1.5," http://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf, 2012.

[35] UIDAI, "Aadhaar Technology Strategy," http://uidai.gov.in/images/AadhaarTechnologyStrategy_mar2014.pdf, 2014.

[36] UIDAI, "Aadhaar Product Document," http://uidai.gov.in/images/AadhaarProductDoc_mar2014.pdf, 2014.

Published by UIDAI Technology Center
Bengaluru, Karnataka, India.