MAIN MENU

Home
About UIDAI
Aadhaar
Aadhaar Usage
Aadhaar Enrolments
Finance and Budget
Consultations
Legislation and Guidelines
Awareness and Communication
Tenders
Vacancies in UIDAI

OTHER ITEMS

RTI
Parliament Questions
FAQs
External Links

RESOURCES

Aadhaar Technology
Biometric Devices
Certified Biometric Devices
Archives
UIDAI Documents
Press Release

AADHAAR STATUS

Check your Aadhaar Status

Features of the UIDAI Model

The Aadhaar will only provide identity: The UIDAI's purview will be limited to the issuance of unique identification numbers (Aadhaar) linked to a person's demographic and biometric information. The Aadhaar will only guarantee identity, not rights, benefits or entitlements.

A pro-poor approach: The UIDAI envisions full enrolment of the residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars that the Authority plans to partner with in its first phase such as – the Mahatma Gandhi National Rural Employment Guarantee Scheme (NREGA), Rashtriya Swasthya Bima Yojna (RSBY), and Public Distribution System (PDS) – will help bring large number of the poor and underprivileged into the UID system. The UID method of authentication will also improve service delivery for the poor.

Enrolment of residents with proper verification: Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the Authority plans to enrol residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is clean right from the beginning of the program. However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they will have access to. The Authority will ensure that the Know Your Resident (KYR) standards do not become a barrier for enrolling the poor, and will devise suitable procedures to ensure their inclusion without compromising the integrity of the data.

A partnership model: The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI will be the regulatory authority managing a Central ID Repository (CIDR), which will issue Aadhaar, update resident information and authenticate the identity of the residents as required.

In addition, the Authority will partner with agencies such as central and state departments and private sector agencies, who will be 'Registrars' for the UIDAI. Registrars will process Aadhaar applications, and connect to the CIDR to de-duplicate resident information and receive Aadhaar. The Authority will also partner with service providers for authentication of identity.

The UIDAI will emphasize a flexible model for Registrars: The Registrars will ensure significant flexibility in their processes, including issuing cards, pricing, expanding KYR verification, collecting demographic data of residents for their specific requirements, and in authentication. The UIDAI will provide standards to enable Registrars to maintain uniformity in collecting certain demographic and biometric information, and in performing basic KYR activities. These standards will be finalised by the KYR and biometric committees constituted by the Authority.

Process to ensure no duplicates: Registrars will send the applicant's data to the CIDR for de-duplication. The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to minimise/eliminate duplicates in the database.

The incentives in the UIDAI system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India provides scope to individuals to furnish different personal information to different agencies. Since de-duplication in the UIDAI system ensures that residents have only one chance to be in the database, individuals are made to provide accurate data. This incentive will become especially powerful as benefits and entitlements are linked to Aadhaar.

Online authentication: The Authority will offer a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority will support Registrars and Agencies in adopting the Aadhaar authentication process, and will help defining the infrastructure and processes they need.

The UIDAI will not share resident data: The Authority envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of the residents they enrol if they are authorised to do so, but will not have access to the information in the Aadhaar database. The UIDAI will answer all requests to authenticate identity only through a 'Yes' or 'No' response. The Authority will also enter into contracts with Registrars to ensure the confidentiality of the information they collect and store.

UIDAI ECOSYSTEM

RESIDENTS

What is Aadhaar
Why Aadhaar
How to enrol for Aadhaar
Check Your Aadhaar Status
Enquiries and Grievances

BUSINESSES

Tender News
Tender Categories
Contracts Awarded
Tender Archives

REGISTRARS

Engagement of Registrars
Registrar and Enrolments
Training
Testing & Certification Portal
Aadhaar Portal
Aadhaar Governance Award

AUTHENTICATION

Authentication Overview
Operating Model Overview
Authentication Service Agency
Authentication User Agency
Authentication Devices
Aadhaar Enabled Payments
More

FINANCIAL INCLUSION

Reports
Notifications
Empanelment of Banks

Data Transparency: The authority will place all the aggregated data for public to access under RTI. However Personal Identity Information (PII) will NOT be accessible by any entity.

Technology will undergird the UIDAI system: Technology systems will have a major role across the UIDAI infrastructure. The Aadhaar database will be stored on a central server. Enrolment of the residents will be computerised, and information exchange between Registrars and the CIDR will take place over a network. Authentication of the residents will be online. The Authority will also put systems in place for the security and safety of information.

Top

Application Architecture

Entities and Roles

UIDAI

The Authority will issue Aadhaar and set standards for enrolment and authentication, to be universally followed. Initially, UIDAI will design, develop, and deploy the Aadhaar Application with the help of service providers. Subsequently, the entire operation will be expanded and operated by an external service provider. In addition to providing the product and services, the UIDAI is also responsible for recruiting Registrars, approving enrolment agencies and providing a list of introducers among others. To further enhance the mission, UIDAI will also help in the creation of services that depend on the Aadhaar authentication.

Registrars

These are public and private organisations that are currently engaged in providing services to the residents, and which operate on behalf of the UIDAI to provide UIDAI services (such as enrolment) to their constituents. For example, profiles of Registrars include state governments, ministries and departments in the Central Government, banks and other financial institutions, telephone companies, etc. While Registrars may provide UIDAI services to all residents, they are not required to do so. Registrars may collect documentation – such as proof of residence, and proof of identity from residents. Registrars are required to store such documents, and have them available for later investigation/audits. Registrars may also receive and have access to some of the data specifically collected by the UIDAI, e.g. demographic data and photograph of the resident. Registrars may store the Aadhaar in their systems, as well as print it on artefacts provided to the resident (such as a card, or a letter). Certain Registrars may store biometric data such as fingerprint, and iris image in a secure manner on smart cards for offline authentication purposes. This data may not be stored on their servers or used for online authentication. To ease the process of registration for the marginalised sections of society, Registrars may provide a list of introducers who may introduce residents thus waiving certain proofs, as required by the KYR document. This list of introducers is Registrar specific. Registrars are also authenticators, and use the authentication interfaces to confirm the details for residents who may have already enrolled in UIDAI system.

Sub-Registrars

These are departments or entities that report to specific Registrar. For instance, the line departments of the state government such as the Rural Development and Panchayati Raj (RDPR) department would be Sub-Registrars to the state government Registrar.

Enrolment Agency

An agency contracted by the Registrar, subject to certification by the UIDAI, to perform their duties. Enrolment agencies provide operators and supervisors for the enrolment stations on the field, and also create the necessary conditions for the optimal enrolment of residents. Enrolment agencies must collect demographic data prior to an enrolment drive. They must notify residents and UIDAI, of the enrolment schedule in advance. Enrolment agencies may be empanelled by the UIDAI for the assistance of the Registrars. However, the Registrars, will be free to engage any other enrolment agencies as well.

Introducer

An Introducer is a well known person authorised by the UIDAI or by a Registrar to introduce individuals for enrolment. This mechanism was specifically created to allow the UIDAI system to reach out to the marginalised and excluded residents who may not have sufficient documentation to meet the proof of identity or address specified in the published KYR norms. Hence, an introducer provides an assurance that the individual applying for an Aadhaar is indeed a resident, and to the best of his/her personal knowledge who they say they are. Registrars may provide a list of introducers with their name and Aadhaar. For various Registrars, we expect that this list will include officials (elected, gazetted and

others), school teachers, headmasters, anganwadi workers, etc. The UIDAI may seek the help of NGOs and other civil society organisations to provide additional Registrars to improve the coverage for the marginalised groups. A carefully crafted enrolment strategy to reach out to the marginalised section of society will depend on a strong, reliable introducer network – that will have to be crafted ahead of time.

Resident

Residents of India, who wish to obtain an Aadhaar, are expected to provide appropriate documentation to meet the KYR norms or to be introduced by an appointed introducer. A resident is defined as a natural person, usually residing in India. Residents are expected to truthfully provide information and documentation to meet the KYR norms, or be introduced by an introducer. Further, they are expected to provide biometric information to the UIDAI. They can expect a smooth experience with the enrolment agency, and a swift response to various issues that they may have. Residents will have access to their data, and the ability to identify when they were authenticated (for a period of time). Access to data of other residents is to be restricted by the UIDAI.

Authenticator

An authenticator is an agency that uses the UIDAI system to authenticate a resident. Authenticators may use demographic data and/or biometric data in addition to the resident's Aadhaar. The authenticator must use the appropriate form of authentication that provides him/her with the necessary assurance for the transaction. Authenticators must register with the UIDAI and provide an estimated usage (primarily for the provisioning). Authenticators may have presence at multiple locations, at each of which they deploy authentication devices. Authenticators may be billed by the UIDAI for certain service levels. The billing relationship will require additional data. The number of authenticators is an important indicator of the health of the UIDAI system as diverse authenticators imply the availability of diverse services to the residents. UIDAI will also lead the way in enabling the creation of service platforms and standards that will allow authenticators to come on board easily.

Overview of applications hosted in CIDR

The application hosted by CIDR can be broadly categorised into core applications and supporting applications. In the core category we have the enrolment and authentication applications services. While the supporting category consists of applications required for administration, analytics, reporting, fraud detection interfaces to Logistics Provider and Contact Centre and the portal.

The Enrolment Application serves the client enrolment request for providing an Aadhaar. The application orchestrates the enrolment workflow by integrating various sub-systems such as address normalisation, third party de-duplication, and Aadhaar generation. Manual exception workflow is required to resolve enrolment requests that cannot be resolved automatically. Basic letter printing and delivery functionality is available for servicing exceptions to normal workflow.

The Authentication Application provides the identity authentication services. Various authentication request types such as demographic, biometric, simple or advanced authentications are supported by this application. The Aadhaar submitted is used for 1:1 match for the resident's record. The inputs are then matched against the resident information found in the biometric database.

The Fraud Detection Application is deployed to detect and reduce identity fraud. For example, identifying fraud scenarios that the application needs to handle are: misrepresentation of information, multiple registrations by same resident, registration for non-existent residents, or personification as someone else.

The Administrative Application takes care of user management, roles and access control, business process automation, and status reporting. It ensures a trust network across both internal and external entities. The external entities could be Registrars, Sub-Registrars, Enrolment Agencies, Field Agencies, Introducers and Authentication clients. For example, the application is required to manage user accounts for the Registrars or Introducers who vouch for identity of individuals who lack proper documentations. The internal entities could be system administrators, customer service agents or biometric and fraud detection agents. The application will allow administrators to track status of other applications, and provide mechanism to escalate failures or delays.

The Analytics and Reporting Application provides enrolment and authentication statistics for both public and partners. It supports visual representation of statistics and allows drill down at regional levels. All the information available for this application is only at the aggregate level thus, ensuring individual identity is completely protected.

The Information Portal provides administrative and information access for internal users, partners and public. Besides the above application, interface application for Logistics and contact centre are also present in the CIDR.

The Contact Centre Interface application provides query and status update functionality.

The Logistics Interface Application interfaces with the logistics provider for letter printing and delivery. It is used for sending and receiving raw data, sending Aadhar data for letter printing, delivering and

receiving periodic status updates on the inbound and outbound communication.

Biometric Solution

The Biometric Solution Provider (BSP) will design, supply, install, configure, commission, maintain and support biometric components of the UIDAI System. In CIDR, there can be up to three BSPs operating simultaneously. Two biometric components are utilised in the UIDAI System. The biometric components are:

1. Automated Biometric Identification Subsystem (ABIS): ABIS will be used in the Enrolment Server as a part of the multi-modal biometric de-duplication solution. In the early release, ABIS will also be used in the Authentication Server for verification. The ABIS will maintain its own database of proprietary fingerprint and iris image templates for de-duplication (and face templates at the discretion of the vendor), and must be able to respond to verification requests accompanied by fingerprint and/or iris images, as well as ISO/IEC 19794-2:2005 format fingerprint minutiae files. Vendors will work with UIDAI to provide further specification within ISO/IEC 19794-2:2005 to promote interoperability with future verification clients.

2. Multimodal Software Development Kit (SDKs): SDKs will be used in the enrolment client, manual check (for duplicates), authentication server (for later releases) and the analytics module. The SDK may contain signal detection, quality analysis, image selection, image fusion, segmentation, image pre-processing, feature extraction and comparison score generation for fingerprint, iris and face modalities.

The biometric solution components used in the UIDAI system are:

• Multi-modal de-duplication in the enrolment server
• Verification subsystem within the authentication server
• Enrolment client
• Manual checks and exception handling
• Biometric sub-system monitoring and analysis.

The functional requirements of the above mentioned five areas are described, followed by the overall functions of the two biometric components.

UID System Requirements of the Biometric Components

Top

a) **Multi-modal Biometric de-duplication in the Enrolment Server**

Considering the expected size of the de-duplication task, the UID Enrolment server will utilize:

1. Multi-modal de-duplication. Multiple modalities such as– fingerprint and iris image will be used for de-duplication. Face photograph is provided if the vendor desires to use it for de-duplication. While certain demographical information is also provided, UIDAI provides no assurance of its accuracy. Demographic information shall not be used for filtering during the de-duplication process, but this capability shall be preserved for potential implementation in later phases of the UIDAI program. Each multi-modal de-duplication request will contain an indexing number (Reference ID) in addition to the multi-modal biometric and demographic data. In the event of one or more duplicate enrolments are found, the ABIS will pass back the Reference ID of the duplicates and the scaled comparison scores upon which the duplicate finding was based. The scaled fusion score returned with each duplicate found will have a range of [0, 100], with 0 indicating the least level of similarity and 100 as the highest level of similarity.

2. Multi-vendor: The complete multi-modal solutions from more than one vendor will be used. The Aadhaar Application will determine routing of a particular de-duplication request. It may determine to route a particular de-duplication request to more than one biometric solution. If it routes a de-duplication request to more than one solution, it is responsible for determining the final outcome of the de-duplication request. The UIDAI ABIS API specifies the interaction between UIDAI Application and ABIS.

The middleware included in the UIDAI application (being developed by ASDMSA) is meant to provide vendor independence and standardisation. The key features of the middleware are:

• Routing and mediation.
• Guaranteed delivery
• Fault tolerance and load balancing
• Open standard based messaging (AMQP) using open source Rabbit MQ
• Transparent connectivity to analysis and system monitoring modules of UIDAI applications
• Support of Web 2.0 based UIDAI ABIS API and CBEFF data format standard
• Encapsulation and isolation of ABIS components

(b) **Verification Subsystem of Authentication Server**

In the first release of the UIDAI server, the biometric verification module, provides verification within the

authentication server. The solution should be capable of 1:1 verification comparisons of enrolled references with incoming ISO/IEC 19794-2-compliant fingerprint, iris or face images or ISO/IEC 19794-2 compliant fingerprint minutiae sets without proprietary extended data.

For the purpose of distributed authentication by UIDAI at a later stage, the biometric verification module may be constructed using SDK. While the functionality of the verification subsystem will not change, the internal architecture may change. The templates will be maintained in memory resident database by the UIDAI authentication server application (not in scope of BSP). If the incoming requests contain a biometric image, the authentication server will use SDK to extract the feature. SDK will also be used to generate comparison score of the sample. The decision for distributed authentication will rest with UIDAI and will be binding on the BSP.

Partner Portal

The UIDAI project is based on a partnership model consisting of Registrars and their respective enrolling agencies on the ground. There are other entities such as device suppliers, trainers, letter delivery agencies, pre-enrollers etc all of whom play an important role in enrolling 1.2 billion residents. The partner portal will cater to the needs of the partner community.

This portal will provide them with overall statistics that involve them, as well as allow them to track individual cases.

These users will be able to track:

• Administration and user management – creation / deletion of the user records
• Aggregate pre-enrolment statistics – number, latency, validation issues. (for Registrars, Sub-Registrars, and Enrolment Agencies)
• Aggregate enrolment statistics – number, latency, approvals, rejection reasons (for Registrars, Sub-Registrars, and Enrolment Agencies)
• Aggregate authentication statistics – number, latency, success / failures (for authentication clients)
• Track individual resident information – pre-enrolment, enrolment, and authentication – that they are involved in.

Public Portal

The UIDAI being a project of national importance will need to continually share various design, development, implementation and operational aspects with the public. The grievance redressal system also needs to be integrated into the public portal to redress complaints and grievances faced by residents in the process of enrolment and authentication. The UIDAI information portal will address the above needs. This portal will also provide all users with information about the UIDAI system, and allow them to drill down on the performance by region, etc. It will not allow users to track individual cases.

However, a method will be provided to get in touch with the UIDAI for specific questions as well as addressing grievances.

All users will be able to view the following:

• List of Registrars, Enrolment Agencies, etc.
• Number of UIDs issued by time (day, month, year), and region (country, state, district, city)
• Performance Metrics – At an aggregate level – the number of Registrars, latency to allocate UIDAIs, number of complaints, etc.
• Authentication requests – count, latency, success /failures.

• Grievance requests filed with the UIDAI and the responses.

Data Portal: We want to expose all publishable public information through a "Data Portal" where all data is exposed in machine readable formats. This portal allows third party developers to develop Web 2.0 applications based on this data.

Registrar System: Registrars will have their own IT infrastructure to interact with Aadhaar System. The functionalities include the following:

• Getting updates during enrolment process
• Uploading bulk demographic data
• Act as an Authentication User Agency (AUA)

As we have seen earlier, a copy of the enrolment data flows from the Enrolment Stations to the Registrar System. The CIDR also updates the Registrar System with the assigned Aadhaar.

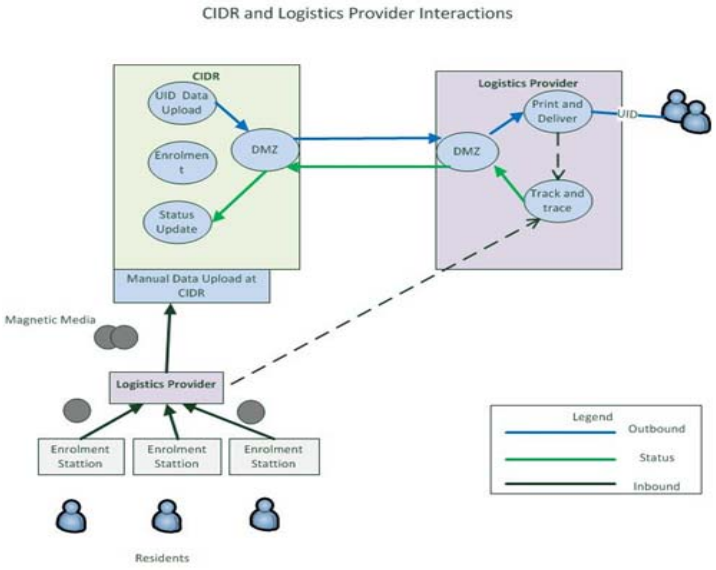
To keep the confidentiality of the data being sent to the registrar system, the data will be encrypted using the public key provided by the Registrar. It follows that the Registrars have to manage their <Private Key, Public Key> pair securely and put the necessary infrastructure in place. The interacting Registrar systems have to be hardened. UIDAI may provide security guidelines to Registrars to assist in the implementation but the ownership will always reside with the Registrars. UIDAI will define interfaces for the Registrar System to interact with CIDR. There will be no libraries to be integrated with. Since the Registrars also maintain a copy of their enrolment data, they have to take enough precautions to secure the data. In order to integrate Aadhaar authentication with applications like PDS, NREGA or similar applications in private sector, UIDAI will provide a library of API using which the new applications can be developed and deployed.

Logistics

Logistics service will be provided by Department of Posts. There are two parts to this:

(i) Inbound Logistics – to receive the raw enrolment images + data in magnetic media and through the network from the Regional Offices or Facilitation Centre. All the incoming data is processed by the CIDR DMZ Application.

(ii) Outbound Logistics – Delivering the UIDAI to applicants and getting the Status Update



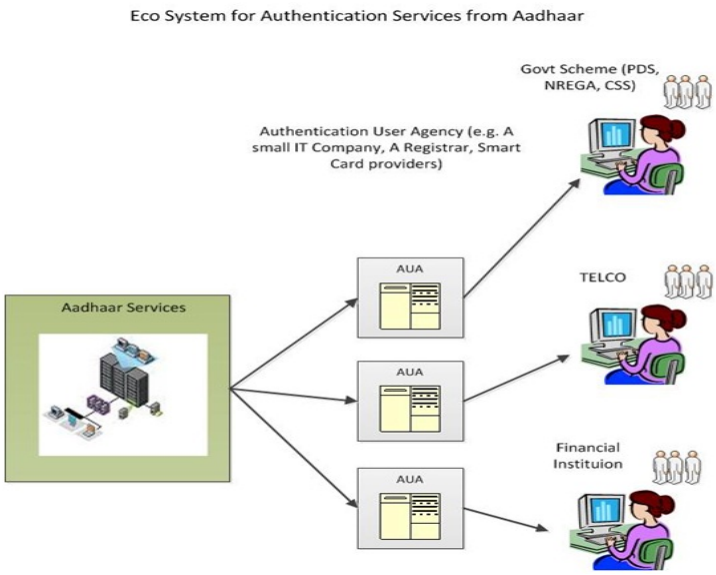
Responsibilities of Logistic Service Provider includes the following:

• Logistics setup for enrolment agencies to send the enrolment data/manifest to the RO/data centre
• Provide printing infrastructure and connectivity to the CIDR. The printing infrastructure electronically receives the Aadhaar allocation letter to be printed and mailed to the enrolled residents
• Mail the printed Aadhaar letter to the enrolled resident
• Provide an online track and trace system to track the status of the enrolments and Aadhaar generation
• Support the call centre provider to track the enrolment status

Top

Security and Infrastructure Technology

Authentication User Agency



Contact Centre

The Contact Centre provides a central point of contact to residents and other entities that will partner with UIDAI during the enrolment and post enrolment stages. The Contact Centre will provide services in multiple languages for residents, Registrars, enrolment agencies and resident service agencies. The service provider for Contact Centre will setup, operate and maintain the Contact Centre including the agents. The service provider for Contact Centre will be expected to:

• Scale operations at the required pace to match volumes of interactions
• Provide analytics support to UIDAI
• Assist in driving performance improvements
• Take end to end responsibility of driving resolution of queries and services
• Analyze the various interactions with the stakeholders, identify and develop process models

The RFP for Contact Centre contains the detailed requirements for Contact Centre. Please refer to this document from UIDAI website. UIDAI has selected Intellinet as the service provider for setting up and operating the Contact Centre. The Contact Centre Architecture diagram is shown below:

Top

UBCC and Research

Introduction The UIDAI has been setup by the Government of India with a mandate to issue a unique identification number to all the residents in the country. A key requirement of the Aadhaar is to

minimize/eliminate duplicate identity to improve the efficacy of the service delivery. Biometrics features are selected to be the primary mechanism for ensuring uniqueness.

No country has undertaken to build a national registry at the scale and accuracy as UIDAI initiative. Nature and diversity of India's working population adds another challenge to achieving uniqueness through biometrics features. Like other technology fields such as telecommunication, we do not have experience like developed countries to leverage for designing UIDAI's biometric systems. For example, the largest existing biometrics database in the world is one order smaller in magnitude than India's needs.

Therefore, it is necessary to create a UIDAI Biometrics Centre of Competence (UBCC) that focuses on the unique challenges of UIDAI.

Mission

To design biometrics system that enables India to achieve uniqueness in the national registry.

The endeavour of designing such a system is an ongoing quest to innovate biometrics technology appropriate for the Indian conditions.

Goals

The mission of UBCC can be achieved through the following distinct goals:

• Specifications: UBCC will specify the initial biometrics system and will enhance the features at regular intervals to insert new technologies and best practices.
• Characterisation: UBCC will evaluate and characterise technology, devices, algorithms and processes to assess what and when specifications need to be revised or enhanced.
• Innovation: UBCC will push the state of art in Biometrics to achieve UIDAI's objectives.
• Assistance: CIDR will be a national resource to other departments for implementing UIDAI compatible biometric systems.

Strategy

UBCC will achieve its goals through the following four-pronged strategy:

• Talent: It will attract and hire world-class biometric talent. UBCC will emphasise quality over quantity and build a small group of exceptional scientists and engineers.
• Collaboration: It will closely collaborate with other technical departments, academic institutes, international experts and international bodies to assimilate and share combined knowledge. It will promote joint research, investigation and analysis at national and international academic institutes through grants and "funded research".
• Rapid adoption: It will build reference architecture, prototype and conduct proof of concept to support rapid adoption of the technology for UIDAI system both during the initial development and later during operation. It will stay grounded by working closely with the operational UIDAI system personnel.
• Biometric Laboratory: It will build and maintain state-of-art laboratory to remain viable independent research and engineering unit.

Top