Aadhaar Handbook for Registrars

January 2013

Unique Identification Authority of India
Planning Commission, Government of India

Contents

1. Introduction

The inability to prove identity is one of the biggest barriers preventing the residents of India from accessing benefits and subsidies provided by Indian government. There is no nationally accepted, verified identity number in the country that can be used with ease and confidence by both the residents and agencies. Different service providers also often have different requirements in the:

- Documents they demand from the residents
- Forms that require filling out
- Information they collect on the individual.

Such duplication of effort and identity silos increase the overall cost of identification and cause inconvenience to the resident. Any process that uniquely identifies a resident and ensures instant identity verification would help:

- Reduce transaction costs
- Transform delivery of a host of social welfare programs
- Help eliminate duplicate identities and fraud.

The savings on this account can be immense and today when states are fiscally stressed, freeing up of resources would provide the desired flexibility in either extending the welfare net or increasing the benefits under the existing programs or simply improving the fiscal situation .

Keeping the above in mind, the Unique Identification number (Aadhaar) has been conceived by the Government of India as a means for residents to clearly and uniquely verify their identity anywhere in the country.

This handbook is meant to:

- **Give an overview of Aadhaar, the process to generate Aadhaar numbers.**
- **Use its authentication services and update it on an ongoing basis**.

Detailed process manuals, which are or will be available on the UIDAI website, may be referred for implementation.

Previous attempts at building 'unique' databases have been beset by quality issues and challenges in the lack of consistent implementation. This project therefore has defined detailed guidelines and templates for the same; especially keeping in mind that Aadhaar will be built through a network of Registrars and enrolment agencies dispersed across the country. The success of the project will be strongly determined by the quality of data collected; as such all partners may therefore keep in mind the need to adhere to these guidelines.

As our partners, Registrars are requested to share feedback extensively and engage with the UIDAI in making this a robust and successful exercise. The handbook and the manuals will be updated on the basis of feedback and will be posted on our website on a continuous basis.

2. Aadhaar Overview

Aadhaar is a 12-digit unique number which the Unique Identification Authority of India (UIDAI) will issue for all residents. The number will be stored in a centralized database and linked to the basic demographics and biometric information – photograph, ten fingerprints and iris – of each individual.

Aadhaar-based identification will have three unique features:
a) Universality, which is ensured because overtime Aadhaar will be recognized and accepted across the country and across all service providers.
b) Every resident of India is entitled to the number.
c) The number will consequently form the basic, universal identity infrastructure over which Registrars and Agencies across the country can build their identity-based applications.

3. Features and Benefits

Aadhaar, which means 'foundation' in many Indian languages, has the following Features and Benefits:

1. **One Aadhaar = 1 beneficiary:** Aadhaar is a unique number, and no resident can have a duplicate number since it is linked to their individual biometrics; thereby **identifying fake and ghost identities** which result in leakages today. Savings from eliminating duplicates and fakes through Aadhaar-based identification will enable government to expand benefits to other eligible residents.
2. **Portability:** Aadhaar is a universal number, and agencies and services can contact the central Unique Identification database from anywhere in the country to confirm a beneficiary's identity.
3. **Inclusion of those without any existing identity documents**: A problem in reaching benefits to poor and marginalized residents is that they often lack the identification documents they need to receive State benefits. The 'Introducer' system, which has been approved for data verification for the UIDAI, will enable such residents to establish an identity.
4. **Electronic benefit transfers:** UID-enabled-Bank-Account network offers a secure and low cost platform to directly remit benefits to residents without the heavy costs associated today with benefit distribution. The leakages in the current system are also stemmed as a result.

5. **Aadhaar-based authentication to confirm entitlement delivered to the beneficiary**: UIDAI offers online authentication services for agencies who wish to validate a resident's identity; this service enables confirmation of the entitlement actually reaching the intended beneficiary.

6. **Improved services through increased transparency:** Clear accountability and transparent monitoring significantly improves access and quality of entitlements to beneficiaries and the agency alike.

7. **Self-service** puts residents in control: Using Aadhaar as an authentication mechanism, residents should be able to access up-to-date information about their entitlements, demand services and redress their grievances directly from their mobile phone, kiosks or other means. In the case of self-service on the resident's mobile, security is assured using two-factor authentication (i.e. by proving possession of the resident's registered Mobile Number and knowledge of the resident's Aadhaar PIN). These standards are compliant with the Reserve Bank of India's approved standards for Mobile Banking and Payments. (Please see Annexure 7.1 for how mobile phone can be used for Aadhaar enabled applications).
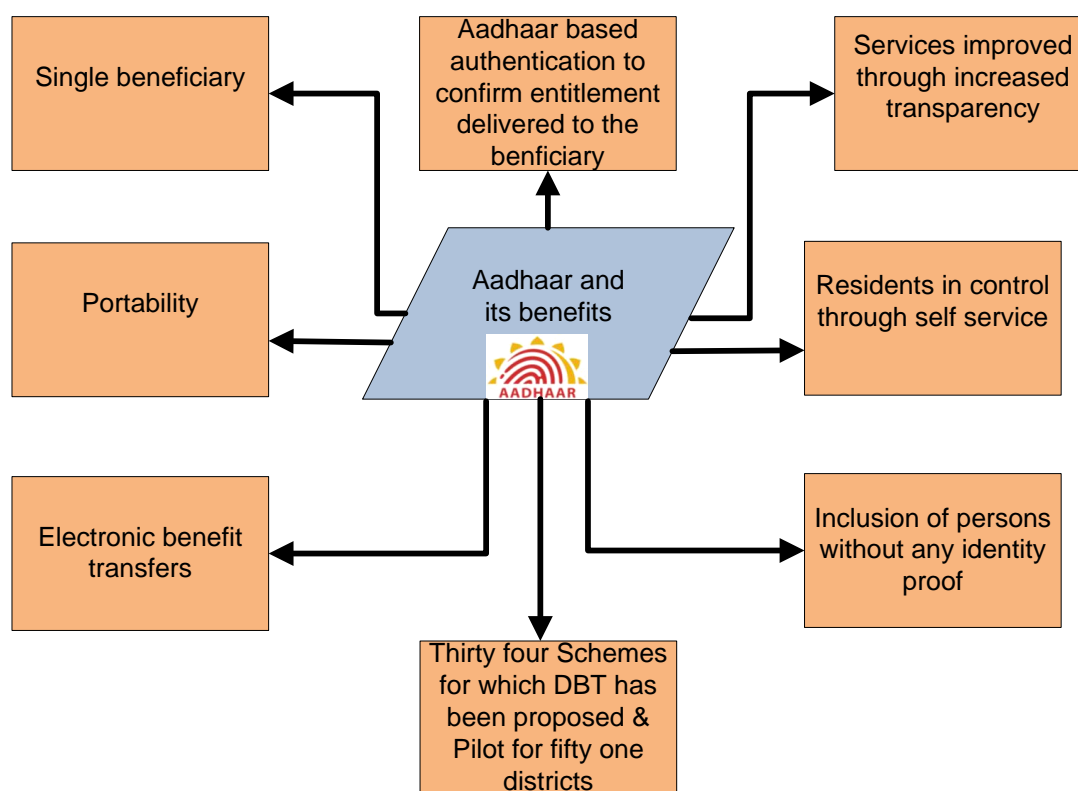

Figure 1: Benefits with Aadhaar

Aadhaar-Enabled Applications

Aadhaar can be used in **any system which needs to establish the identity of a resident and/or provide secure access for the resident to public services including welfare services/benefits** offered by the system. Aadhaar can be used in the delivery of the following applications:

- **Direct Benefit Transfers -** A total of 34 schemes for which DBT have been proposed & pilot of 51 districts for 18 schemes are deployed. The direct benefit diagram lists down some of the benefits being transferred to residents.
- **Food & Nutrition** – Public Distribution System, Food Security, Mid Day Meals, Integrated Child Development Scheme.
- **Employment** – Mahatma Gandhi National Rural Employment Guarantee Scheme, Swarnajayanti Gram Swarozgar Yojana, Prime Minister's Employment Guarantee Program.
- **Education** – Sarva Shikhsha Abhiyaan, Right to Education.
- **Inclusion & Social Security** – Development of Primitive Tribe Groups, Indira Gandhi National Old Age Pension Scheme, Indira Awas Yojana.
- **Healthcare** – Rashtriya Swasthya Bima Yojana, Janashri Bima Yojana, Janani Suraksha Yojana, Aam Aadmi Bima Yojana.
- Other miscellaneous purposes including Property Transactions, Voter ID, PAN Card etc.
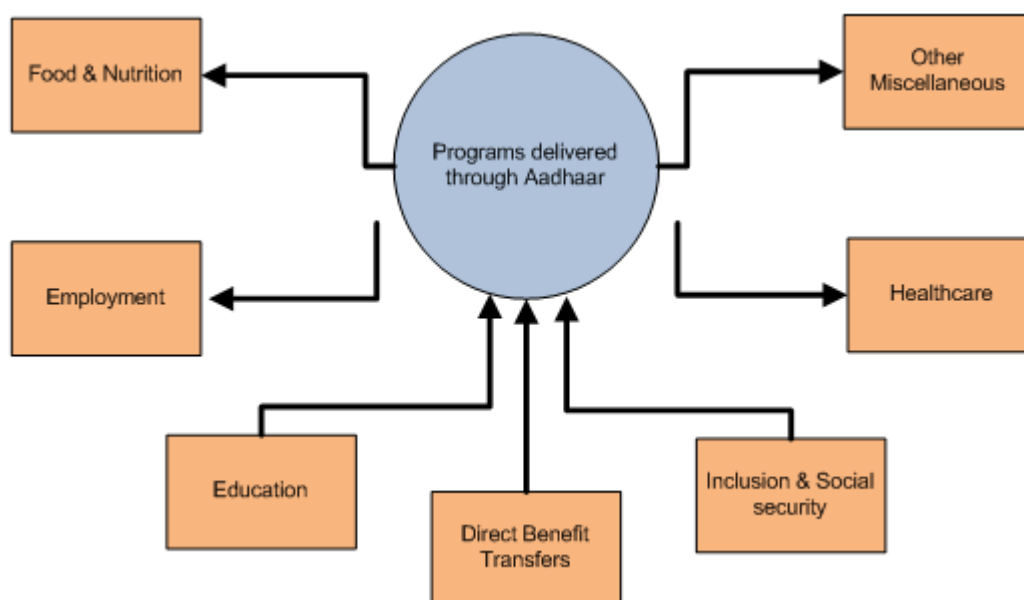

Figure 2: Programs delivered

As per its mandate, the UIDAI will actively work on defining the usage of Aadhaar numbers across applications and services, in partnership with concerned Registrars and Agencies.
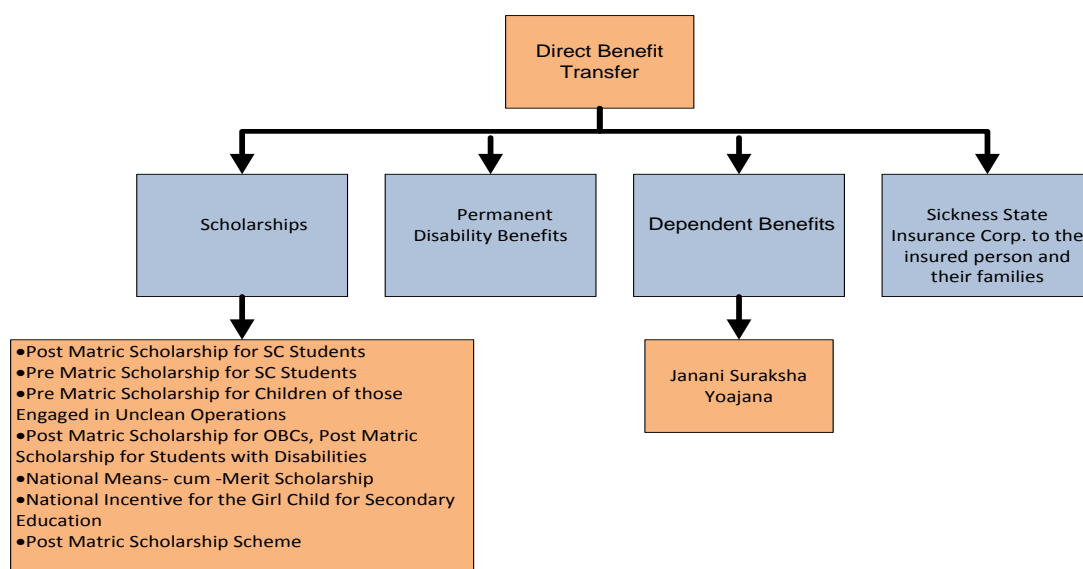
Figure 3: Direct Benefit

Integration of Aadhaar brings **two primary benefits to the Registrar** and agencies:

1. **De-duplication:** Since UIDAI will ensure that the same resident will not be issued two Aadhaar numbers, these numbers are truly unique and can be used to de-duplicate, integrate existing databases or create new ones.

2. **Authentication:** At the time of delivering a service to the resident, UIDAI recommends that :
   a. The Aadhaar number is captured along with a biometric (one or more fingerprints, iris), verified online with UIDAI and the service delivered only to the valid resident.
   b. In situations where the biometric is not available or the need for authentication is not as high, demographic data along with the Aadhaar number can be verified with UIDAI, and used as a more basic verification. UIDAI does not guarantee the authenticity of the resident in this case.

Thus, Registrars who partner with the UIDAI to enroll residents can integrate Aadhaar numbers into their programs (referred here as applications), to leverage the benefits of Aadhaar from day 1 of starting operations. These benefits will accrue as soon as enrolment starts – in the form of de-duplicating the existing databases and removing fake/ghost identities. In addition, benefits of substantially larger scale can be realized if Aadhaar number and Aadhaar based authentication is integrated into the Registrar's existing systems to track and accurately deliver benefits to targeted residents.

However, State governments need not wait to develop their customized applications before starting the enrolment process. Registrars can integrate Aadhaar –based authentication at a later date also, by re-designing their systems and processes to include the Aadhaar ID and Aadhaar based authentication.

See Annexure 7.2 for details of Aadhaar-enabled state applications.

Benefits of Online over Offline Authentication

Currently the delivery of benefits is authenticated through offline systems – in many cases, a physical ID card that's issued to a beneficiary and increasingly through smart cards which carry additional authentication details tagged to a beneficiary. In contrast, Aadhaar offers real time, online authentication. The following table offers a comparison of offline and online authentication methods:

Issues	Offline	Online
Addresses duplicate records		
Information	Resides in "smartcard"	Resides in " virtual card"
Business application	Resides in each device	Resides online in the backend cloud
Device Type	Complex, expensive	Simple, inexpensive
Cost and lifecycle management	High	Low
Flexibility to add applications	Difficult	Easy
Interoperable/choice	X	✓
Real/time	X	✓
Fraud Detection and analytics	Difficult	Easy
Any Device(Incl. mobile)	✓	✓
Can work without connectivity	✓	X

It is evident from the above that Online authentication will prove to be beneficial over the lifecycle of the program and offer far greater flexibility, inter-operability across programs and fraud detection at far lower costs.

4. How will Aadhaar be built?

Aadhaar will be built in partnership with Registrars. Registrars will collect demographic & biometric data from residents directly or through Enrolment Agencies. Aadhaar will be issued by the UIDAI to residents after de-duplication of data. Financial support will also be provided for Registrars to operationalise this program as per approval of the Government of India from time to time. The Government had initially

approved 20 crore enrolments in pilot phase till March 2012. Another 40 crore enrolments across 18 States/ UTs have been approved (Refer Annexure 7.3 for List of approved 18 States/UTs - for Enrolments by UIDAI's Non-RGI Registrars). These enrolments are to be done by UIDAI's non- RGI Registrars over the next 18-24 months starting April 2012.

5.What is the Aadhaar Ecosystem?

The UIDAI has identified the following partners and defined processes for Registrars to commence operations:

1. **Registrars:** To collect demographic & biometric data from residents directly or through Enrolment Agencies. They will be adhering to the UIDAI developed standards, procedures and processes, guidelines and technology systems to execute the entire Aadhaar enrolment process. They can also collect additional data which will be referred to as KYR+ fields for various applications.
2. **Enrolment Agencies:** To enable quick on-boarding of enrolment agencies, UIDAI has empanelled enrolment agencies across all States and Union Territories. These agencies have been categorized by technical and financial strength and the list is available on our website under the 'Registrars & Enrolments' tab.
3. **Device Certification Agency:** To support Registrars in deploying the right devices for the enrolment process, UIDAI has appointed STQC (Standardization, Testing & Quality Certification) as the device certification agency. STQC will certify biometric devices (Fingerprint Scanner & Iris Camera) by make & model.
4. **Training & Certification Agencies:** To bring all enrolment operators to a uniform skill level, UIDAI has built standardized training content, empanelled Training Agencies that are authorized to deliver our training and appointed Sify and MeritTrac as the Testing & Certification agency.
5. **Agency for Document Management:** UIDAI has appointed HP for managing hard copies of resident's documents collected during enrolment process.
6. **Financial Institutions:** UIDAI has signed MoUs with various Banks who will open UID Enabled Bank Accounts (UEBA). This will not only pave the way for financial inclusion of marginalized residents, but also offer significantly lower cost channels for Registrars to transfer financial benefits directly to residents. UIDAI's approach on Financial Inclusion is in line with Financial Inclusion targets & strategy outlined by RBI & GoI.
7. The UIDAI is also working with a number of **public and private sector organizations to UID-enable their application** so that the residents start accruing comprehensive benefits.
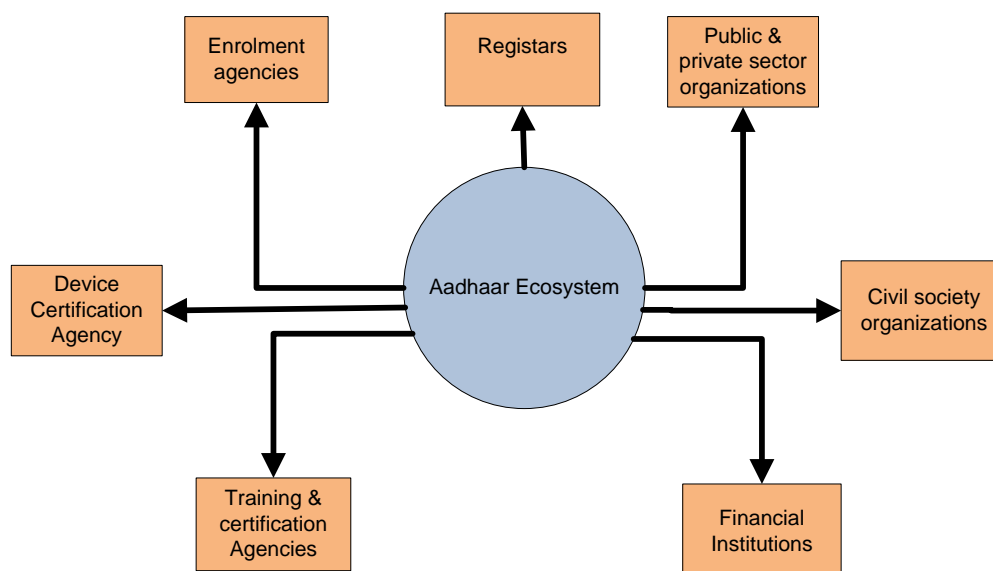
Figure 4: Aadhaar Ecosystem

UIDAI has also defined detailed '**Registrar On-boarding Process'** and '**Registrar Roles and Responsibilities' documents** in order to support Registrars across the stages of becoming Aadhaar Ready.

6. Becoming Aadhaar Ready

For becoming Aadhaar ready, UIDAI recognizes/ authorizes an entity known as Registrars for the purpose of enrolling the individuals for UID numbers. Registrars are typically departments or agencies of the State Government/Union territory, public sector undertakings and other agencies and organizations, which interact with residents in the normal course of implementation of some of their programs, activities or operations. Examples of such Registrars are Rural Development Department (for NREGA) or Civil Supplies and Consumer Affairs Department (for TPDS), insurance companies such as Life Insurance Corporation and Banks. Please refer Annexure 7.4 for list of documents for 'Registrar On-boarding Guide & Implementation Support'.

The On-boarding Process of Registrars

1. **Identify Nodal Department** for Aadhaar; set up Apex/empowered committee headed by CM and implementation committee (UIDIC) headed by Chief Secretary; sign MoU. Any Non-State Registrar (NSR) desirous of undertaking enrolments in a particular State/UT will also be co-opted in UIDIC by the UIDAI Regional Office.

2. **Identify Departments which will act as Registrars along with a nodal Officer.** Other Departments which are not included as Registrars in the project at the time of enrolment, will have the option of 'Aadhaar enabling' their systems at a later date.

3. **Identify Agency for receiving financial assistance for enrolment**: The Authority will financially support its Registrars for successful Aadhaar number generation. To operationalise this arrangement, the States will have to provide the Authority, details of the Registrar (name and account details) through which they would like to receive the amount.

4. **Setup Joint Working Group** – headed by the Head of the Nodal Dept/Registrar. The other members should be the Nodal Officers, & members who can lead the Technology, Process, IEC, applications teams from the Registrar's side. UIDAI will nominate appropriate representatives to assist the State Government/Registrars in carrying through the entire process. Bank representatives may be included where the Financial Inclusion (FI) solution is a part of enrolment.

5. A **Project Initiation Workshop** will mark the commencement of the project and include an overview of Aadhaar for the benefit of new entrants into the team, outline the Enrolment and IEC Implementation approach and plan (how and what needs to be done), roles & responsibilities of the Joint Working Group and the high level timelines and project plan. This must be attended by members from the Implementation Committee and the Joint Working Group. See Annexure 7.5 for details of Roles & Responsibilities.

6. A **sensitization training cum workshop** can be setup in parallel for members of the Registrar's organization who need to be aware of the project/plans etc. It is recommended that similar sensitization sessions be organized by the Registrar Department for key functionaries of the district / village level governing bodies and other influencers who can contribute to the success of this project.

7. This will be followed by a **Workshop to define the Enrolment Strategy** and detail the process and technical integration required to start enrolments. This will include the Enrolment Plan, no. of districts and residents to be covered per month and therefore the infrastructure and other requirements to meet the same. This is expected to be attended by the Joint Working Group with optional participation from the Implementation Committee.

8. This will be followed by a set of **sub-group workshops and meetings** with members of the **process, technology, IEC** and **applications** teams respectively to identify the key areas of integration and implement the same.

9. The Registrars are expected to give special attention to **Social Inclusion**. Define the role of Civil Society Organizations (CSOs) in the enrolment process and develop a panel of CSOs at the local level who can help enrol marginalized communities. (refer Annexure 7.6 for more details)

10. A **Go Live readiness Workshop** will be scheduled 2-3 weeks before scheduled 'go-live' date to take stock of the implementation status on items required to start enrolments.
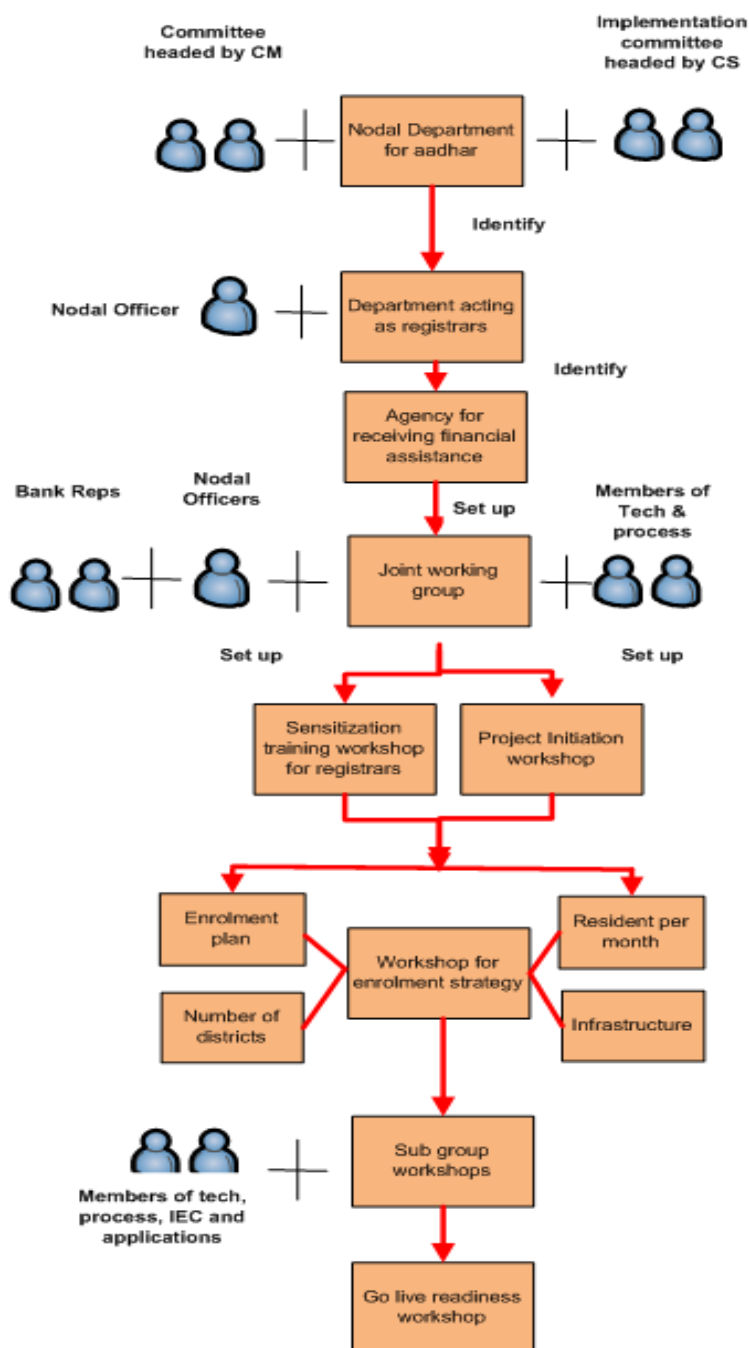
Figure 5: Registrar On-boarding Process

On boarding/ Sign off of Non State Registrars for carrying out resident enrolment registration

The final sign off for on boarding of Non State Registrars will be done by the respective divisions at headquarters in respect of FIs, NSDL and India Post.

Further the process for Non State registrars to carry out resident enrolment registration will be as follows:

1. For working in a refresh phase of resident enrolments, NSR should approach the Nodal Division at UIDAI (HQ) to convey its willingness to work in it.

2. The concerned divisions will advise NSRs to complete Register Readiness Checklist (RRC) and will explain the revised process to NSRs.

3. NSR should send the RRC with the contact details of nodal officers (region wise) to the nodal division at UIDAI Head office.

4. The concerned division will review the RRC and approve/disapprove accordingly.

5. NSR's readiness will be communicated to all ROs from the respective nodal division.

6. Post receiving the information of NSR's readiness from concerned nodal division of UIDAI- HO, ROs will get the RRC from EA's of the NSR and ensure the readiness of the EA's for the enrolments.

7. ROs will have four major functions to perform- a) Approve the enrolment centre's b) Make NSR a UIDIC member in case he/she co-opts c) Sign off on the enrolment agency readiness checklist d) Go ahead for enrolments to the Registrar in particular State/ Region.

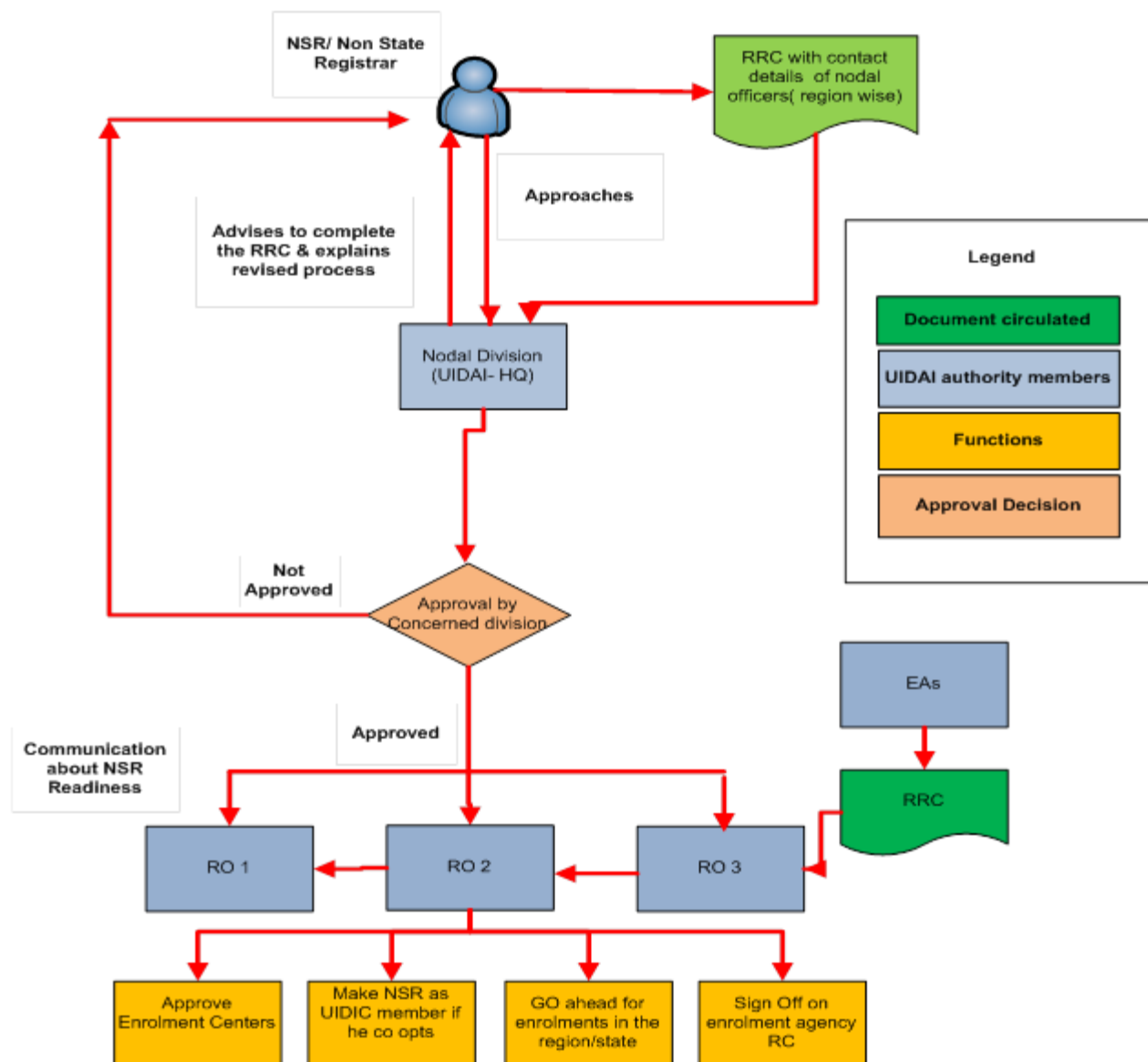Please refer the diagram below for further clarity on the above process.

Figure 6: On boarding of NSR's

Roles and Responsibilities of a Registrar

The **Roles and Responsibilities** of a Registrar can be summarized below:

1. The Registrar is required to **ensure the security and accuracy of data** (particularly biometric data) collected from residents.

2. Registrars may retain the biometric data collected from residents enrolled by them, if they have clearly articulated strategy for safe custody and utilization of these enrolment packets. The **Registrar will have to exercise a fiduciary duty of care with respect to the data collected** from residents and shall bear liability for any loss, unauthorized access to and misuse of data in their custody.

3. In order to ensure data integrity and security, the **biometrics captured shall be encrypted** upon collection by using the encryption key defined by the Registrar. The UIDAI has defined **security guidelines for the storage of biometric data** in order to give some guidance to the Registrar. The Registrar shall have to define their own **security policy and protocols to ensure safety of the Biometric data**. In the interest of transparency, it is recommended that the Registrar inform the resident that they will be keeping the biometric data and also define how the data will be used and how it will be kept secure.

4. The **Registrars must retain the Aadhaar Enrolment/Correction Form, copy of Proof of Identity / Address/Date of Birth/Relationship and Consent for enrolment documents** in proper custody till the time they are handed over to the UIDAI appointed agency for document management.

5. **In case of disputes with respect to enrolment of residents, the Registrar is required to co-operate** with UIDAI in resolving the matter and shall provide access to necessary background documents and other matters of evidence necessary to resolve the dispute.

6. The Registrar is required to support the UIDAI in conducting **audits and checks on the enrolment process** and follow the directions of the UIDAI in order to make the system compliant with the UIDAI enrolment framework.

7. **NSR will keep UIDAI Regional Office (RO) informed of enrolments** within their own premises. Engagement in enrolment activities proposed outside their own premises in any particular State will be approved by the State level UIDIC.

8. **Registrars need to define a 'data updation' process** in order to keep the resident data accurate and complete in their respective databases.

9. **Check Pin Code Master -** Registrar should perform the following activities prior to start of enrolments in the region:
   a) Review the pincode master data.
   b) Provide list of PIN codes to be corrected in PIN codes master to UIDAI using existing Pin Code correction process.
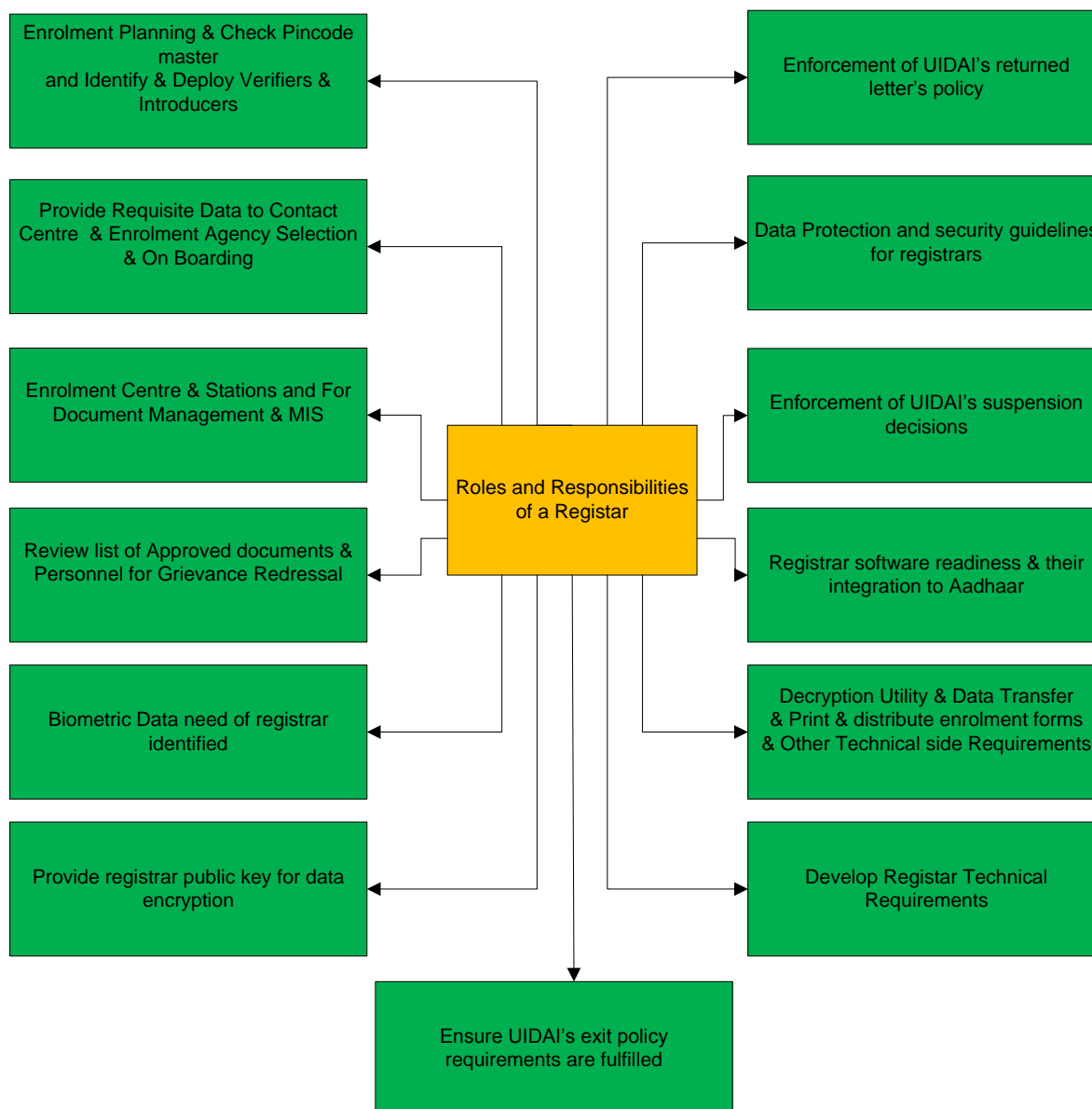
Figure 7: Roles and Responsibilities of a Registrar

Key Policy Highlights

The following is a brief extract of the policy guidelines pertaining to Registrars:

1. **The Registrar is a partner of the UIDAI** in the implementation of the UID project.
2. The Registrar is under an obligation to enroll residents following the **protocols, standards, process and guidelines** laid down by the UIDAI.

See Annexure 7.7 for details of the Legal Framework governing Aadhaar.

Document Storage Guidelines for Registrars

Background

The Unique Identification Authority of India shall issue AADHAAR numbers based on demographic and biometric information provided by the resident.

The demographic information consists of four mandatory fields: Name, Date of Birth, Address and Gender; of which name, data of birth and address are required to be supported and verified by documentary proof of identity, address and date of birth. The purpose of the document storage guidelines is to define the standard procedure of handling documents collected and generated during the resident Enrolment process for AADHAAR numbers. There are several documents which are part of the enrolment process for AADHAAR and each of them need to be handled with care and stored in a manner that will enable ease of retrieval at a later date (if required). The list of documents in the Enrolment process is:

1) Proof of Identity, address and date of birth (some residents may have a single document which can act as proof for all three, while other residents may produce different documents for each)

2) Enrolment form (this form may not be used by all Registrars since some may already have pre-enrolment data available, which will only need to be verified by the resident at the time of enrolment)

3) Consent for enrolment (this form contains details of enrolment and confirmation of details by the resident as well as consent of the resident for sharing of data for welfare and financial services in case of introducer based enrolment endorsement by the introducer)

About the UIDAI DMS initiative

UIDAI has taken initiative for creation, operation and maintenance of Infrastructure for physical storage of Consent letter and accompanying documents pertaining to Proof of Address and proof of Identity produced by residents during Aadhaar Enrolment and their conversion and storage into digital format. The proposed infrastructure called the "Aadhaar Document Management System" for UIDAI will have following features:

1) Physical storage of Consent letter and accompanying documents produced during enrolment process.

2) Scanning & conversion of physical forms and documents into digital/electronic formats and proper storage supported by state of the art Document Management System.

3) Easy, convenient, safe & secure retrieval of original forms & documents when needed.

Basis of Pickup

The pickup unit will be on the basis of batch ID.

One EID set of documents= All papers for an individual

One Batch= EID sets from a single machine with recommended size of 250 EID sets

1 Pickup will consist of one Manifest consisting of 50, 000 EID sets (approximately, +/-10%)

Role of registrars

Documents produced by residents are handed over during enrolment process to the enrolment agency appointed by registrars and later the same documents are submitted back to registrars for further processing and storage.

Registrars are responsible for collecting and securely storing all the documents submitted by residents during enrolment till the UIDAI appointed DMS service provider collects document from registrar offices and provide receipt of the same. Registrar may authorize enrolment partner to handover the documents directly to DMS Agency for physical pickup. However the Registrar holds the responsibility for coordinating the same with all other terms & conditions for pickup mentioned in this document. Following table describes the roles and responsibilities of registrar.

Legend P = Primary Responsibility, S = Secondary Responsibility

Best Practices for Document Storage

An enrolment document carries important and confidential resident information. UIDAI urges to handle Enrolment documents with care and protect it from damage and theft. This section outlines some best Practices for document handling at various stages are listed below:

1. During enrolment, keep documents in a tray and do not fold them.
2. Upon completion of enrolment, immediately collate the set of documents and staple it at left hand corner.
3. Store documents in proper box and avoid folding and excessive stacking.
4. Protect documents from direct sun light, inflammable material, dust and water. It is recommended to use plastic covers to store set of documents to protect against environmental hazard
5. Transport documents from enrolment center to registrar office only in properly sealed boxes tagged with proper manifest and packing list

6. Avoid writing on documents as this may create confusion for operators in later phases of the process.
7. Avoid tying up documents using rope or packing tapes directly, this will permanently damage documents. If tying up is unavoidable use PET Straps with edge protectors.

Registrar Office (DHQ)

1. Store documents/boxes indoor in a secured place to protect from fire, water and sabotage.
2. Keep the documents/boxes in a lockable place with proper ventilation till pickup by DMS service provider
3. Avoid movement of documents from storage area for quality check or master manifest preparation purpose
4. Avoid de-stapling, re-stapling or folding or excessive stacking of documents, it is recommended to store document in boxes

Note: List of District Head Quarters with code number to be used during sending a pickup request.

Please refer Annexure 7.8 for the list of documents for verifying POI, POA and DOB.

Guidelines for Financial Assistance

1. In order to reduce the financial burden of implementing Aadhaar, the Authority has been provided funds by the Central Government to assist the Registrars at a rate approved by the Government of India from time to time. To operationalise this arrangement, the States will have to provide the Authority, with details of the Registrar (name and account) through which they would like to receive the assistance.
2. Assistance will also be provided to develop ICT infrastructure; specifically for integrating existing software applications of partner agencies, procurement of hardware and software, engaging consultants / resource persons to advise partner agencies , engaging software agencies, developing cloud applications at the national level for the large scale social sector schemes and providing integration support.   Details of the program are available on our website.

Enrolment Process

Setup & Preparation

In order to start enrolments, the Registrar has to complete the following activities, many of which can run in parallel and would have commenced post the Project Initiation Workshop:

1. **Enrolment Planning** – As a part of the Enrolment Planning workshop, the Registrar is advised to finalize the targeted enrolment nos., locations to be covered and timelines for the same. This data can in turn be used to plan the no. of Enrolment Stations needed, locations for the same, devices needed, operators to be staffed etc. It is strongly recommended that the Registrar enroll all residents of the locality and not limit it to their beneficiaries/ customers. **'Sweeping' all residents will give Registrars the benefits of economies of scale** and optimizing on the cost of enrolment per resident. However, the Registrars can identify districts, in a phased manner, for the launch of Aadhaar enabled services and focus on enrolment sweep in these districts rather than spreading the entire effort thinly across the State/UT.

2. **Define KYR+ fields** if any are to be collected and initiate technology integration with respect to data capture API and logistics. Also finalize if **pre-enrolment data** from existing databases are to be used during enrolment. The **Aadhaar Application Software** for enrolment should be ready for deployment. See Annexure 7.9 and 7.10 for details of 'Technology Overview' and 'Pre-enrolment data and KYR+ data Integration' respectively.

3. **Identify Enrolment Agencies** – Registrars can consider using only agencies from the list empanelled by the UIDAI or they may identify through other sources. If Non-Empanelled Agencies are used, UIDAI strongly advises that these agencies be subject to same terms and conditions of work which apply to the empanelled agencies.

4. **Subcontracting has serious impact on the quality and security of data. Agreement with enrolment agencies should have conditions to discourage sub-contracting.** Model RFP/Q templates and the list of empanelled agencies have been published on the UIDAI portal.

5. **Detailed station deployment plan** needs to be uploaded by Enrolment Agency and approved by the Registrar using an online mechanism developed by UIDAI. **Online appointment scheduling** should be encouraged for better crowd management at the centers.

6. **Procure infrastructure and equipment including biometric devices** as per standards defined by the UIDAI for setting up an enrolment centre through the designated enrolment agencies.

7. It is recommended that the **Registrar must insist on Enrolment agencies using only Operators/Supervisors** who have been trained, certified and their Aadhaar numbers have been generated. Operators/Supervisors may be trained using the modules / agencies that the UIDAI has empanelled for Enrolment Operator training; alternatively, the Registrar can ask operators to cover the modules in 'self-study' mode and appear for the test directly. All Enrolment

Operators need to be tested and certified, keeping in mind the significant impact they have in collecting good quality and accurate data from residents. See Annexures 7.11 & 7.12 for details of the Training modules.

8. Registrars must **Review Pin Codes** in Aadhaar Client Master Data and get Pin Code information corrected and completed prior to starting enrolments in their area.

9. **Print and distribute Aadhaar Enrolment/Correction Forms.** Registrars can have a separate form for capturing KYR+ data.

10. Define an integrated **Information, Education & Communication Plan & Material** leveraging the content developed by the UIDAI. The UIDAI's IEC guidelines list in detail the different kinds of stakeholders to engage (PRI members, introducers, influencers etc.) and the recommended messages and media to use for each of them. The IEC plan lists the activities to be triggered 45/30/15/ 7 days before commencing enrolments. See Annexure 7.13 for details.

11. Registrar should also **identify an Officer to whom all relevant grievances may be forwarded**; and two senior officers for managing escalations of the same. The Joint Working Subgroup should also develop probable queries / grievances that can come from the beneficiaries & correct responses for them; finalize the process & turnaround time for responding to the queries/grievances.

12. Before enrolments start, Registrars will need to **identify Introducers** who can help enroll beneficiaries who lack PoA/PoI documents. They can also **leverage CSOs to better reach marginalized residents, act as Introducers,** and **build awareness** among them to mobilize enrolments from this group.

13. **Identify Verifiers and ensure their presence at the enrolment centre** during the operational hours of the centre for verifying resident's documents.

14. Finally if **Financial Inclusion solution** will be a part of the enrolment process, then work with the UIDAI to identify Banks to partner with; define processes as required to implement the Financial Inclusion solution.

15. Review the **Enrolment Centre Setup checklist** and verify if all required activities are completed.
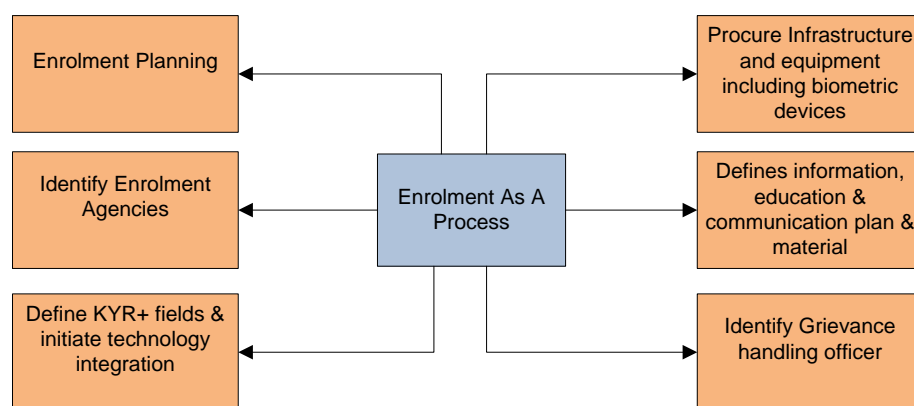
Figure 8: Enrolment as a process

The recommended layout for **Enrolment** is below:

1. The layout should include 'Resident' and 'Operator' seats with work table and waiting chairs for waiting residents. The area captured for the layout is of width 10 feet and of length 7 feet.

Figure 9: Enrolment Office Layout

2. The second enrolment office layout consists of seats for a resident, an officer, a work table and seats for waiting residents. The width of the total area will range around 10 feet with a length spanning to 7 feet.

Figure 10: Enrolment Office Layout 2

Data Capture

The Go-live readiness workshop should have been completed and all requirements verified as met, before a Registrar proceeds to this step.

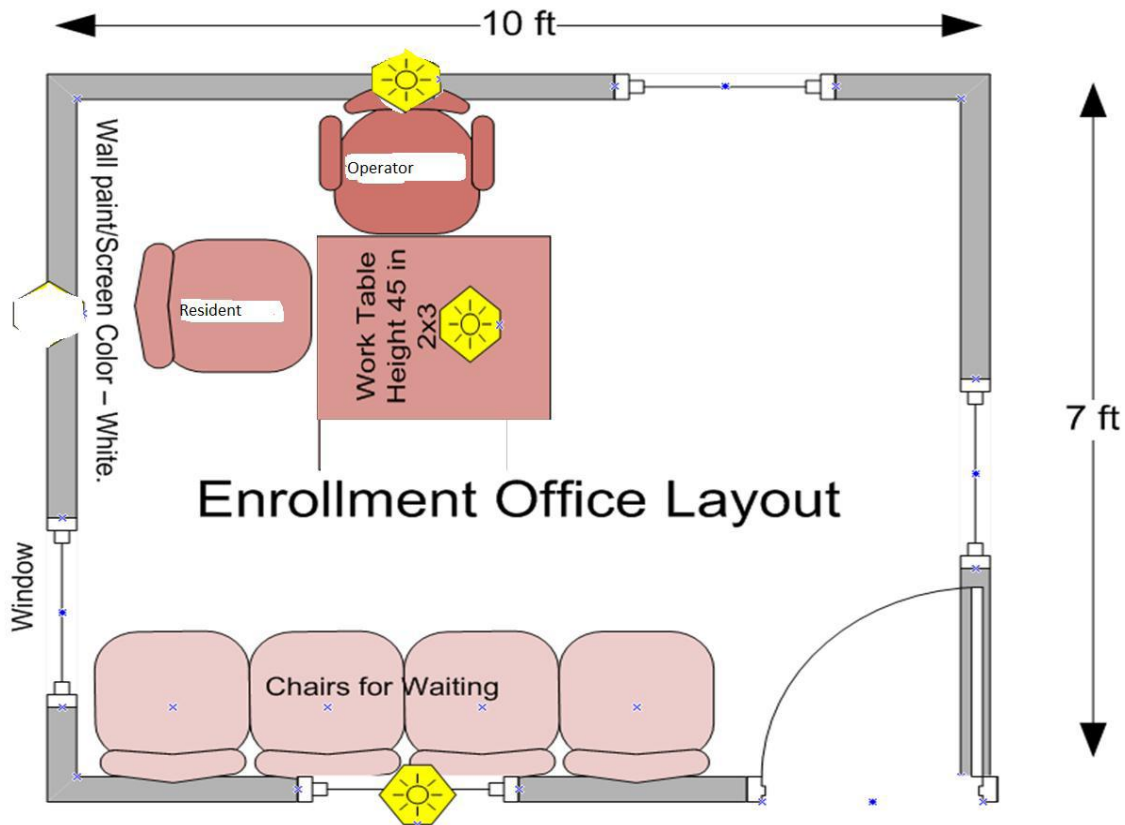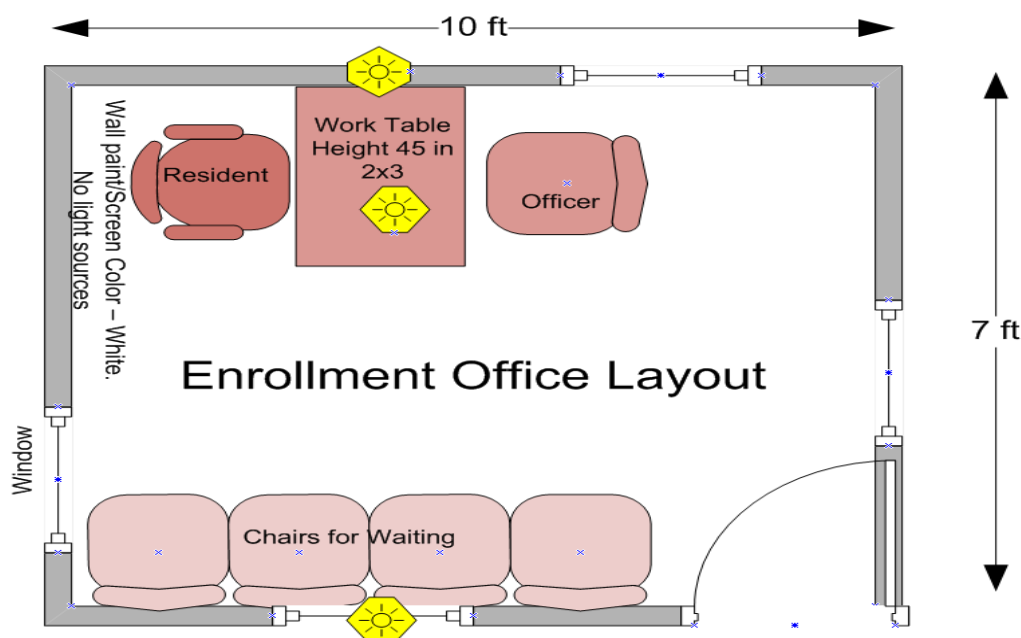After an enrolment centre is ready, Enrolment Agencies can begin the process of capturing residents' demographic and biometric data as follows:

1. **Capture Demographic Data**:
   a. **Aadhaar Enrolment/Correction form (containing KYR fields) and Registrar's KYR+ form (if applicable) is filled by the resident.** The data can also be extracted from a pre-filled database. Filling Aadhaar Enrolment/Correction form is mandatory and will be required - even in case of prefilled data.
   b. **Verify the identity and address** of the resident as per defined standards. The verification methods are basis:
      i. **Document based verification** – where the Proof of Identity / Address/Date of Birth/ Relationship documents are verified by the Registrar's representative.
      ii. **Introducer based** – where Introducers authorized by the Registrar, authenticate the identity and address of the resident.
      iii. **Head of Family based** – where Head of Family endorses family members based on Proof of Relationship Documents.

c. The Operator must check Resident's **consent for Information sharing and Aadhaar enabled Banking services** and record the same.

2. Once demographic data is captured, the operator will proceed to **Collect Biometric Data**:

a. Exceptions if any (missing finger / eye for e.g.) are recorded as per guidelines detailed in the Enrolment Process Manual.

b. Facial Image, Iris and Fingerprints are captured.

Ask **resident to verify if the demographic and biometric data displayed on the screen are accurate**; print consent letter and issue acknowledgment once resident confirms accuracy.

3. **EA then exports data** and transfers to the UIDAI either by uploading the data packets using online sftp mode or by sending the hard disk/memory stick to UIDAI. UIDAI shall soon be discontinuing the practice of receiving data through hard disks and all data must be uploaded through SFTP.

4. **File the documents** for storage with the Registrar and UIDAI Document Management System (DMS). Instantaneous **scanning of resident documents** at enrolment centers and integration with their data packets **will become mandatory from October 2012**.
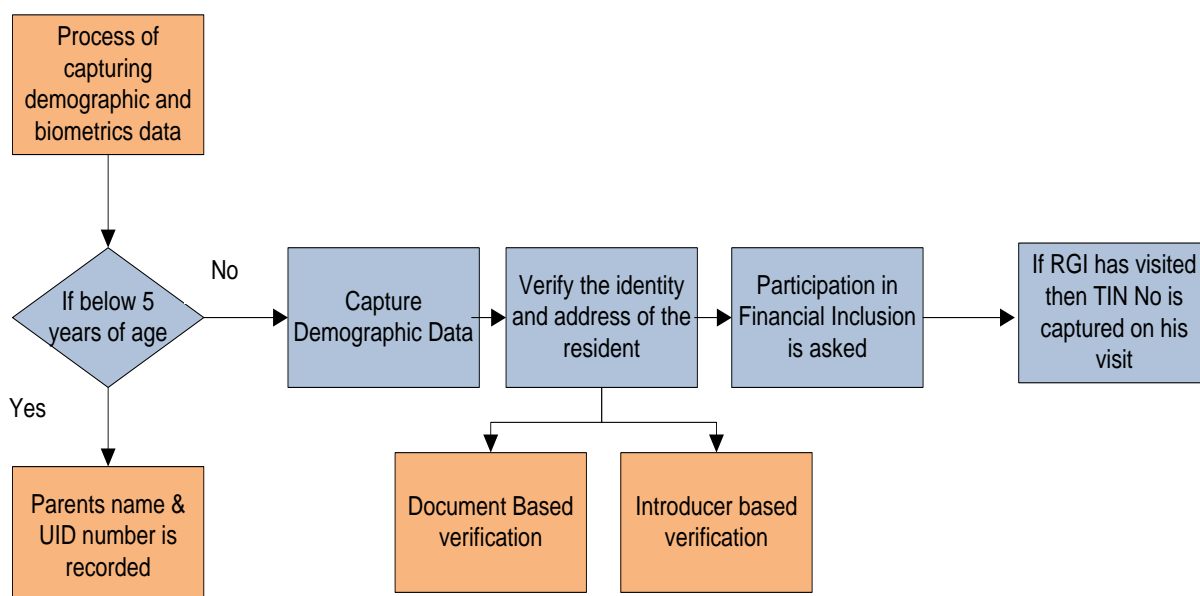
Figure 11: Capturing Demographic Information
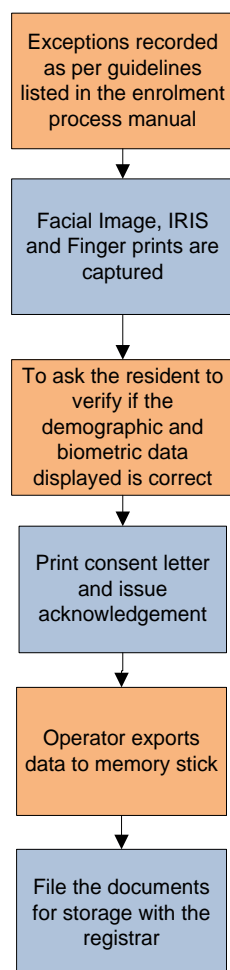
Figure 12: Capturing Biometric information

First Mile Logistics

This process refers to the transfer of digitized enrolment data from the enrolment station to the UIDAI's Central ID Repository (CIDR)

For transferring enrolment data to the CIDR, following options are used:

1. **Direct upload of data to CIDR** - using Aadhaar SFTP client.
2. **Direct upload of data to CIDR** through Hard Disk- using Aadhaar SFTP client.

Data must be uploaded to CIDR within 20 days of enrolment. Beyond 20 days, data packets can be uploaded only via ROs with the Registrar bearing the penalty for a period of 40 days. Beyond 60 days, the packet can be uploaded but the Registrar will not receive any payment for the same.

Monitoring Data Transfer & Recovery of Lost Data: It is expected that each Laptop being used for enrolment will connect to the internet periodically to sync stations with CIDR (Central Identification Data Repository). To enable this, availability of a data stick is mandated.

a. Syncing stations informs CIDR in advance, what data to expect.

b. For the data records successfully received at CIDR, the process for deletion of such data residing at the enrolment station is triggered automatically.

c. In cases where there is a problem with data records received from this enrolment station, a fresh instruction for exporting this data again is generated automatically.

Hence this connectivity, at periodic intervals, is vital to ensure proper housekeeping and management of the data transfer process. **Station Sync must be ensured at least once in ten days.**
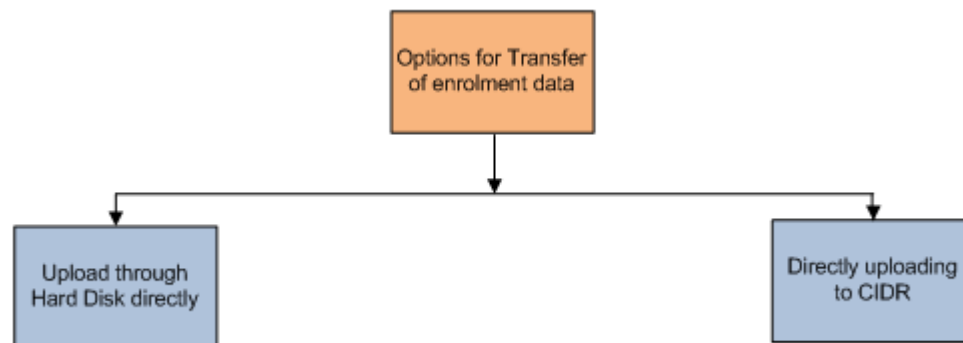
Figure 13: Enrolment data transfer

De-dupe and Aadhaar Generation

This is an automated process run by the CIDR and is described below for reference:

1. Once CIDR receives the enrolment data, it carries out the **necessary quality and validation checks & readies for de-duplication**.
2. **CIDR will run the de-duplication algorithm** to match the details of a resident enrolment request with existing entries in the database. Biometric data in the enrolment record i.e., finger and iris prints will be used for the same to ensure uniqueness.
3. **If no match is found, Aadhaar no. is issued** and letter generated for the same. **If duplicate is found, a rejection Letter is generated** to inform the resident that a duplicate record exists. **If process/data errors are identified, rejection letter is generated** and the resident is asked to re-enrol.
4. Details of the final status on each of the Enrolment Nos. will be shared electronically with respective Registrars and Enrolment Agencies periodically.
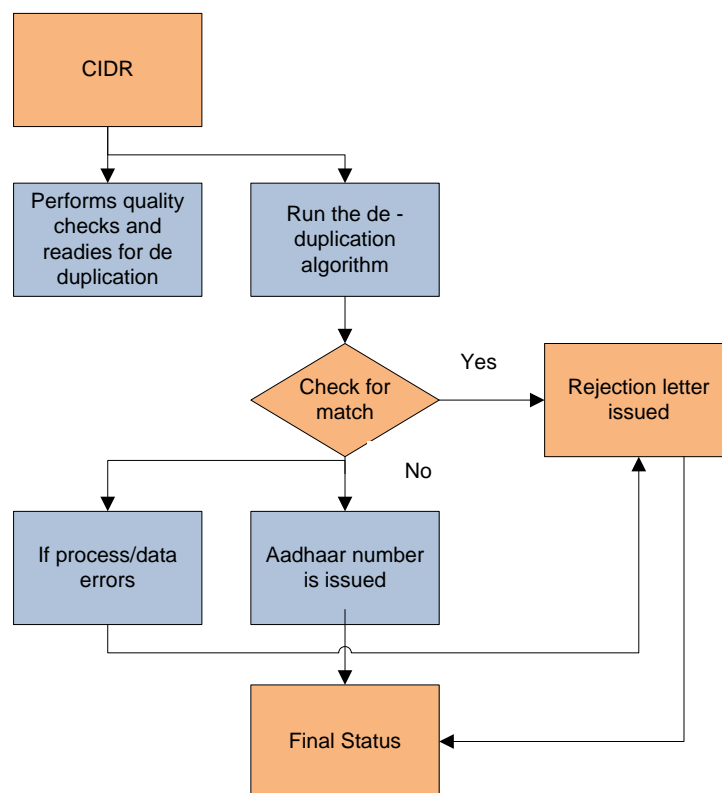
Figure 14: Automated Process for De Dupe and Aadhaar Generation

Last Mile Logistics

This process refers to the **Communication of the Aadhaar Number** to the Resident by means of a letter:

1. All **successful enrolments are communicated through a Letter** to each resident, delivered utilizing the Speed Post Service of India Post. UIDAI may also launch a web based Aadhaar letter facility subject to technical and security considerations.
2. Rejections to the enrolment process are also communicated through a **Rejection Letter**.
3. Undelivered letters are returned to the UIDAI. The resident may request for a letter at a later date by making a request to the Contact Centre.
4. Residents can also check their Aadhaar status directly at website http://www.uidai.gov.in/ using their Enrolment Numbers.
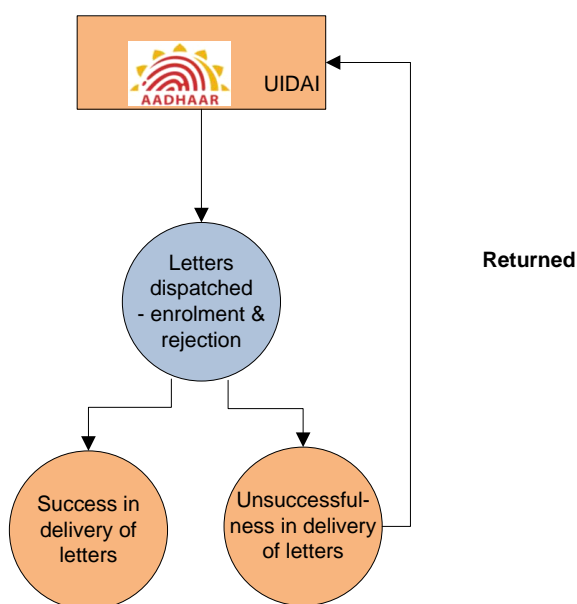
Figure 15: Delivery of Aadhaar letters

Query and Grievance Handling

The UIDAI has setup a **Contact Centre** to manage all queries and grievances and serve as a single point of contact for the organization.

1. The key stakeholders serviced by the Contact Center are Residents, Registrars, Enrollment Agencies, Authentication User Agencies and Authentication Service Agencies.
2. The Channels of Communication are

a. Phone: Toll Free 1800 300 1947. 7:00 AM to 11:00 PM. Monday to Saturday and 8:00 AM – 5:00 PM on Sunday (not available on National Holidays)

b. E-Mail: help@uidai.gov.in

c. Languages Supported: Hindi, English, Marathi, Telugu, Kannada and Bengali.

3. There are two operational sites of contact center one in Pune and the other one in Jamshedpur.

4. Any resident seeking enrollment is given a printed acknowledgement form with an ENROLMENT NUMBER, that enables the resident to make queries about her/his enrolment status through any communication channel of the contact centre.

5. The Contact Centre services Enrolment Agencies/Operators on basic technical queries through a Technical Helpdesk only in English and Hindi language.

6. The Registrar is expected to put in place a Team that would serve to quickly address any matters requiring resolution that may pertain to the Registrar, but may be conveyed to the UIDAI Contact Centre.

7. **Queries / grievances which need Registrar/Enrolment agency involvement will be transferred to the Registrar** appointed Nodal Officer through the following web link here: http://110.234.122.102/aadhar/ui/loginpage.aspx. (For login credentials e-mail may be sent to arajhansuidai@gmail.com). The Time taken for resolutions to be resolved is to be finalized jointly.

Data Updation Process

The UIDAI has defined broad guidelines at this stage for the updation of demographic and biometric data collected during enrolment, which are as follows:

1. **Demographic data updations** will be required if there was an error in enrolment or when a resident changes his address / name etc. **Biometric data updation** will be required for children, and other residents in case of accidents / other loss.

2. The data updation process for demographic data will be a simple process involving document verification standards defined for the enrolment process. Biometric data will also be updated using the same devices and process used for enrolment.

3. Registrars need to maintain atleast a skeletal enrolment network in their respective locations, after the 'enrolment sweeps' are completed to facilitate ongoing updation of their databases. **Long term/Permanent enrolment stations** need to be established by the Registrar at Taluk/Block/Municipality level, so that the residents can continue to enroll even if they have missed the first opportunity. These could be touch points for the residents in case they want to get their data updated.

Details of charges along with further guidelines on the process will be defined by the UIDAI, when this process commences.

Post a request for updation of demographic data, information is supplied to the authorities by:
1. The resident may complete the update request and submit all required documents online.
2. The resident may only complete the data entry part of the update request and send the supporting documents by post.
3. The request along with relevant documents is to be sent by post.

Online Update

Online update of information can be done via Self Service Update Portal (SSUP)- This is a portal for residents with AADHAAR Number, through which they may change/update the information, they have given at the time of AADHAAR Enrolment. Any resident with a mobile number who wish to change/update the details associated with valid reason and document can update their profile using this portal. Resident can update his/her Name, Address, Gender, Date of Birth, Mobile Number and Email ID through this portal. To update the details, resident needs to upload self attested copies of relevant documents.

Performance Monitoring & Audits

A strong monitoring of performance and audit process is critical to drive rigor in the execution of the processes defined above. Keeping in mind the need to have consistent and standardized implementation, the monitoring & audit process will serve as a control mechanism for the UIDAI and Registrars to deliver on the same.

A twofold process is envisaged at this stage:

1. **MIS Analytics & Exception Reports:** the UIDAI will generate a set of standard reports for daily / weekly / monthly monitoring of process performance. Additionally, a set of exception reports will be generated for fraud detection, to flag performance issues etc. Registrars can review the list of standard reports on offer and add/modify to the list.
   These reports can be found in the QC portal meant for Registrars, Enrolment agencies & ROs.

Following is a brief on the kinds of reports fetched from the QC portal.

Kinds of Reports

All the reports related to Quality Assurance are being generated from QA Portal. The different access is provided for the users as per their requirement and they are able to access the reports related to them only e.g. a registrar can access the QA reports related to the Enrolment Operators and Data Packets associated with them. The reports are segregated in nine parts. Home page is a Dashboard of the overall QA Operations.

All the reports being generated on this portal can be viewed in tabular form as well as be exported to an excel sheet. The different types of reports that can be generated from the QA portal can be detailed down below. Usually all reports are one day old.

General Reports
These reports are available for everyone with an access to QA MIS Portal.

- Pending Packets for Manual QA (language Wise)
- Pending Packets (Registrar Wise)
- Pending Packets for Review (RO Wise)
- Packets released from QA (Last 3 days)

QA Operations Report
The following reports are available for QA operations

- QA User Current Status
- QA Operator Wise Report After Review
- QA Operator Date Wise Report Before Preview
- Enrolment Operator Wise Report
- State Wise Pending Report
- Date Wise Receive Pending Report
- RGI Language Wise Pendency

Error Analysis Reports
UIDAI has segregated the Data Errors into 7 categories. This report analyses the Errors made during Enrolment. The report is generated Registrar Wise, EA Wise and Operator Wise. The concerned stake holder can view the reports related to them only.

- Error Type Analysis Registrar Wise
- Error Type Analysis EA Wise
- Error Type Analysis Operator Wise

Regional Office Reports

Error Analysis Report-RO-wise - This report is for UIDAI ROs. The report is available of the EAs state wise falling under different ROs.

Registrar Reports

These reports are accessed by Registrars.

- Error Analysis Report Registrar EA Wise
- Registrar EA Operator Wise
- Reg. EA Opt. Wise Report (Registrar EA Operator Wise)

EA Reports

These reports are accesses by EAs

- Error Analysis Report EA Registrar Wise
- Error Analysis Report EA Operator Wise

Quarterly Error Reports

These reports are available for all the stakeholders to analyze the quality of their data. The reports are available Registrar Wise and Registrar Agency Wise.

- Registrar Wise
- Registrar Agency Wise

RGI Reports

These reports are available for RGI and stakeholders associated with RGI e.g. Registrar and EAs. The following three reports are available currently for RGI.

- RGI Registrar and Agency Wise Report
- RGI QA Error Analysis
- RGI Registrar and Operator Wise Report

2. **Audits:** In addition to MIS based monitoring, the UIDAI will conduct sample audits in the entire gamut of enrolment, training, logistics, grievance resolution and updation processes for controllership purposes. It is recommended that Registrars setup a similar process to audit the performance of Enrolment Agencies and other partners they engage with.

As a part of strategy review, it has been decided that demographic and other errors like biometric mix up, process violations would invite **Penalties which would be deducted from the amount payable to the Registrar every month**. UIDAI will share details with the Registrars who will be required to make detailed enquiries and take follow up action since they have contractual agreements with the enrolment agencies for error free data.

7. Annexures

7.1 Use of Aadhaar enabled Applications on the mobile phone

While Aadhaar-based benefits and service delivery can be made available to residents via agent-assisted kiosks, the Aadhaar secure authentication model will also enable these services to be delivered to residents directly via their mobile phones. This will ensure that residents may securely access their government benefits, track their bank accounts, send and receive money or make payments from the anytime-anywhere convenience of their mobile phones.
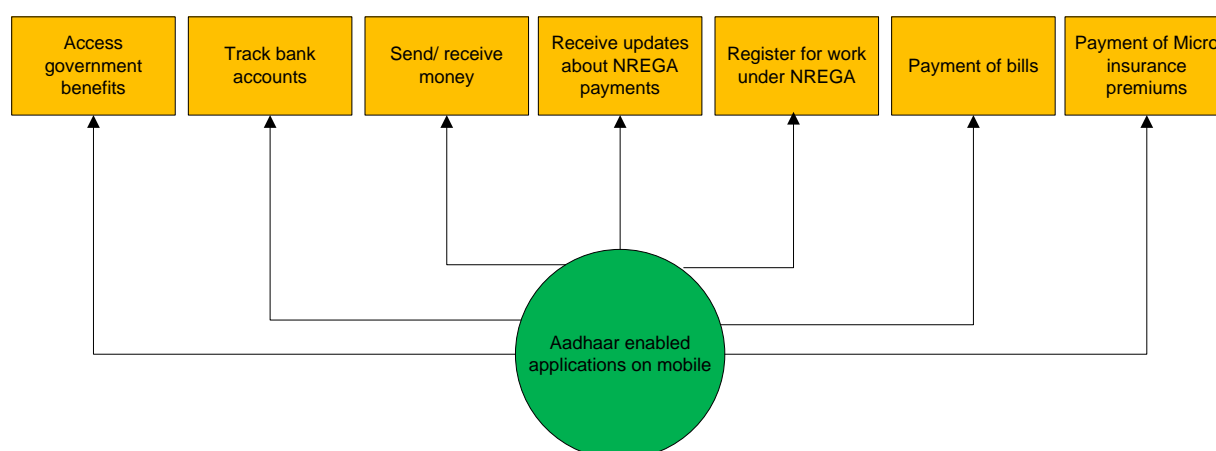

Figure 16: Aadhaar enabled applications on mobile phone

In the beginning these services may be largely informational – such as updates about NREGA payments or bank balances. However it is entirely conceivable for residents to be able to register for work under the NREGA scheme as well as payments of bills, micro-insurance premiums and other money transfer transactions right from their mobile phones. In the case of self-service on the resident's mobile, security is assured using two-factor authentication (i.e. by proving possession of the resident's registered Mobile Number and knowledge of the resident's Aadhaar PIN). These standards are compliant with the Reserve Bank of India's approved standards for Mobile Banking and Payments.

Aadhaar-based micropayments

Aadhaar, which identifies individuals uniquely on the basis of their demographic information and biometrics, gives individuals the means to clearly establish their identity to public and private agencies across the country. Aadhaar, once it is linked to a bank account, can help poor residents easily establish their identity to banking institutions. As a result, Aadhaar makes it possible for banking institutions to provide ubiquitous, low-cost micro-payments to every resident of India.
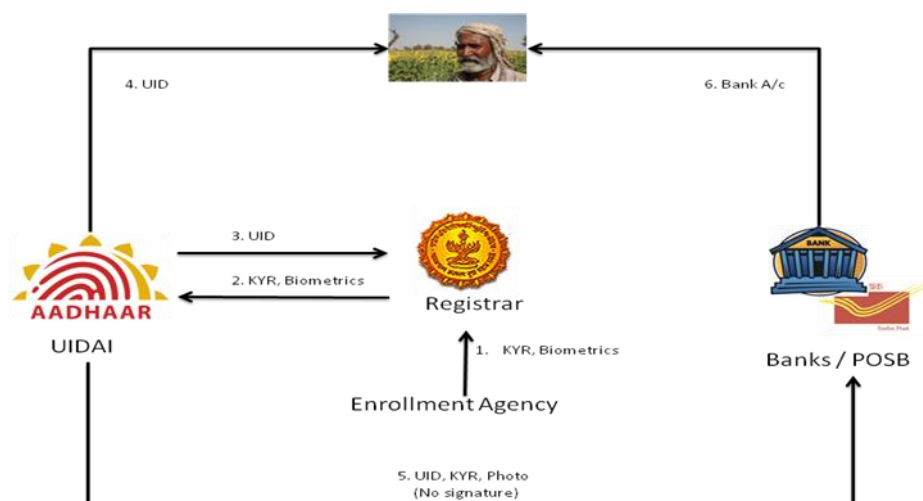
Figure 17: Account opening workflow

UIDAI will facilitate Aadhaar-based micro-payments in two phases:

1. During Aadhaar enrollment, UIDAI will collect information from the resident for the purpose of opening an Aadhaar-enabled bank account. The resident's photograph and demographic data will be sent to a bank to actually open the account.

2. After enrollment, microATMs will be deployed by banks. These handheld devices will make it possible for residents to access their Aadhaar-enabled bank accounts for deposits, withdrawals, remittances, and balance query. The residents will authenticate themselves to the bank by using their Aadhaar number and fingerprint.

It is envisioned that each of India's 600,000 villages will have two microATMs, as Aadhaar enrollment covers the entire country.

Simultaneously, microATMs will also be deployed where the urban poor reside, to bring about urban financial inclusion.

Figure 18: Aadhaar based payments

The key features of UID-enabled micropayments are as follows:

1. **UID KYR sufficient for KYC:** The strong authentication that the UID will offer, combined with its KYR standards, will remove the need for individual KYC (Know Your Customer) verification by banks for basic, no-frills accounts. It will thus vastly reduc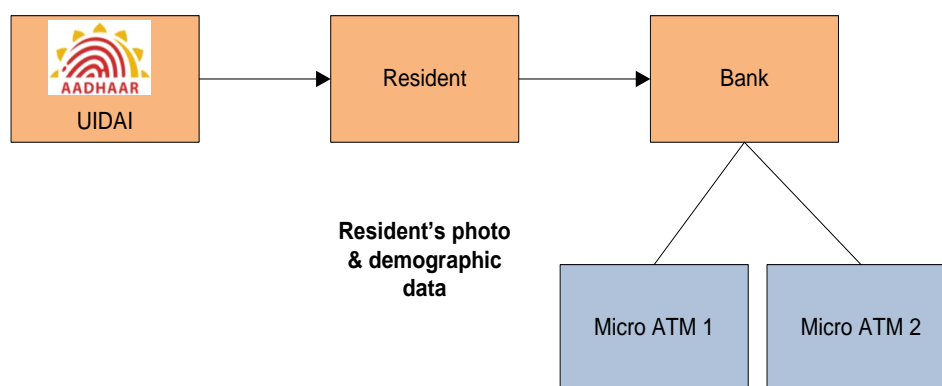e the documentation the poor are required to produce for a bank account, and significantly bring down KYC costs for banks.

2. **Ubiquitous BC network and BC choice:** The UID's clear authentication and verification processes will allow banks to network with village-based BCs (Business Correspondents) such as self-help groups and kirana stores. Customers will be able to withdraw money and make deposits at the local BC.

3. **A high-volume, low-cost revenue approach:** The UID will mitigate the high customer acquisition costs, high transaction costs and fixed IT costs that are now faced in bringing bank accounts to the poor.

4. **Electronic transactions:** The UID's authentication processes will allow banks to verify poor residents both in person and remotely. More importantly, this facilitates direct transfer of benefits (e.g., MNREGA wages, old age pensions) to the resident directly without the incumbent leakages of a manual disbursement system.

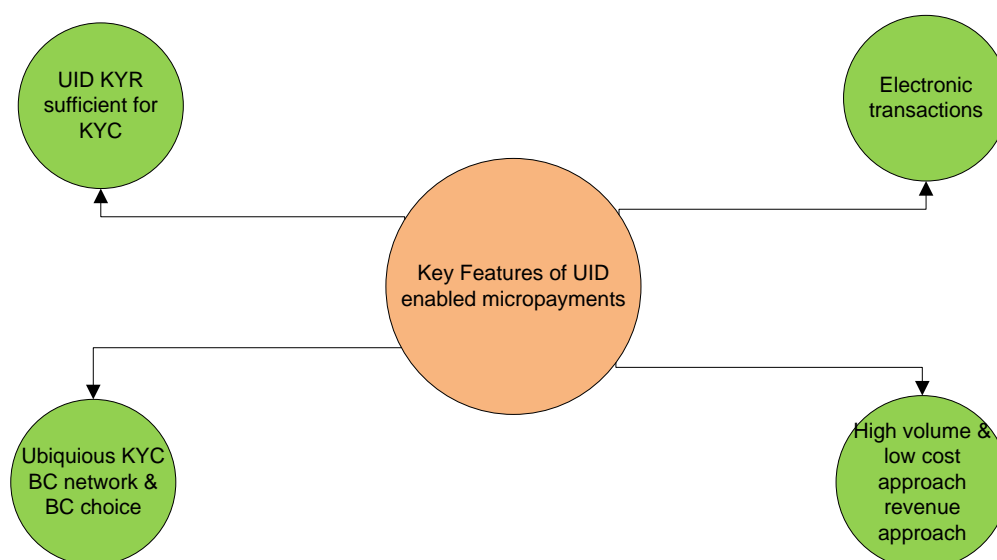Thus, UIDAI will help bring about the national goal of inclusive growth.

Figure 19: Features of UID enabled micropayments

7.2   Details of Aadhaar-enabled Applications

Aadhaar enabled PDS

	Current issues	How Aadhaar can address challenges
1	Duplicate/fake ration cards	Aadhaar biometric de-duplication will ensure unique and genuine beneficiaries
2	Exclusion of residents without proper documents	Aadhaar will provide identity and address proof
3	Leakage/diversion at ration shop or in the supply chain	Resident authentication can ensure targeted and guaranteed delivery of ration Aadhaar-based authentication to track food grain movement
4	Managing food-grain storage and ensuring timely distribution	Online Aadhaar authentication can help in real-time knowledge of demand, consumption and help optimize supply chain management
5	Lack of choice	Aadhaar authentication is not restricted to any one shop, providing choice and portability of benefits to residents
6	Not integrated with other food security linked programs such as ICDS, mid-day meals	All food benefits can be linked to the UID number and integrated into an "online nutrition account"
7	Lack of flexibility to change benefits	Aadhaar enabled online system can allow for changes in entitlements to be made efficiently, especially in emergency situations
8	Difficulty in monitoring	Aadhaar linked MIS system can help in better monitoring at the state level, community level and by residents and CSOs
9	Grievance handling and fraud analytics	Aadhaar authentication could enable fast grievance reporting through mobile or online channels

Aadhaar-enabled public health system

	Current issues	How Aadhaar can address challenges
1	Exclusion of residents without proper identification documents	Aadhaar will provide identity and address proof
2	Tracking doctor and nurse attendance	Online Aadhaar authentication could help in real-time confirmation of doctor, nurse presence in the PHC
3	Leakages in medicinal supplies	Aadhaar authentication will guarantee deliver of medicines to correct beneficiaries reducing leakages
4	Lack of healthcare records	Aadhaar enabled online patient healthcare record can help in efficient and effective diagnosis of patients
5	Integration with health insurance programs	Aadhaar ID, authentication and healthcare records can be integrated with health insurance programs
6	Grievance handling and fraud analytics	Aadhaar auth could enable fast grievance reporting and resolution through mobile or online channels

Aadhaar-enabled SSA

	Current issues	How Aadhaar can address challenges
1	Duplicate/fake beneficiary lists	Aadhaar biometric de-duplication will ensure unique genuine beneficiaries per school
2	Exclusion of residents without proper identification documents	Aadhaar will provide identity and address proof
3	Tracking teacher and student attendance	Online Aadhaar authentication could help in real-time confirmation of teacher, student presence in the classroom
4	Lack of choice and mobility	Aadhaar authentication is not restricted to any one school providing choice and mobility to the residents
5	Leakages in scholarships, grants	Aadhaar authentication and FI platform will ensure guaranteed and targeted delivery of benefit
6	Lack of monitoring student enrolments/drop-outs	Aadhaar enabled MIS system can help track students and performance better
7	Integration with other student-centric benefit programs	Can help integrate student-benefit programs such as ICDS, mid-day meals, bicycle programs, girl child programs
8	Grievance handling and fraud analytics	Aadhaar authentication could enable fast grievance reporting through mobile or online channels

Aadhaar-enabled MNREGA

	Current issues	How Aadhaar can address challenges
1	Duplicate/fake beneficiary lists	Aadhaar biometric de-duplication will ensure unique genuine beneficiaries
2	Exclusion of residents without proper identification documents	Aadhaar will provide identity and address proof to seek job cards
3	Difficulties in demanding work	Work can be demanded by using Aadhaar authentication through mobile or kiosk enabling timely employment or unemployment wages
4	Attendance at work sites	Aadhaar authentication will guarantee worker presence at work site and improved accountability on the work supervisor
5	Lack of choice and mobility	Aadhaar authentication is not restricted to any one area providing choice and mobility to the residents
6	Payments	Aadhaar enabled micropayments platform could help in efficient payment of wages through microATMs/BCs
7	Grievance handling and fraud analytics	Aadhaar auth could enable fast grievance reporting and resolution through mobile or online channels

Aadhaar-enabled Pensions/other direct payments (JSY, NOAPS, NMBS, subsidies, loans, insurance, others)

	Current issues	How Aadhaar can address these
1	Duplicate/fake beneficiary lists	Aadhaar biometric de-duplication will ensure unique genuine beneficiaries
2	Exclusion of residents without proper identification documents	Aadhaar will provide identity proof

	Current issues	How Aadhaar can address these
3	Payments happen through distant bank branches or agents	Aadhaar enabled micropayments solution will take the bank account to residents and help them make or access their payments in a secure environment guaranteed by biometric authentication
4	Leakages in payments through postal service	Aadhaar authentication at the time of money order delivery will ensure guarantee in receiving funds
5	Integration and monitoring	Various schemes can be linked and monitored centrally, by residents and community by using a Aadhaar enabled central MIS system
6	Lack of choice and mobility	Aadhaar authentication is not restricted to any one area providing choice and mobility to the residents
7	Grievance handling and fraud analytics	Aadhaar authentication could enable fast grievance reporting and resolution through mobile or online channels

7.3   List of approved 18 States/UTs - for Enrolments by UIDAI's Non-RGI Registrars

Following is a consolidated list of 18 states for enrolments. In these 18 states, there are a set of nodal officers residing with registrars. Relevant information regarding both can be found in the link here: http://uidai.gov.in/registrar-link-2.html

Sl.No.	States/UTs
1	ANDHRA PRADESH
2	CHANDIGARH
3	DAMAN & DIU
4	GOA
5	GUJARAT
6	HARYANA
7	HIMACHAL PRADESH
8	JHARKHAND
9	KARNATAKA
10	KERALA
11	MADHYA PRADESH
12	MAHARASHTRA
13	NCT OF DELHI
14	PUDUCHERRY
15	PUNJAB
16	RAJASTHAN
17	SIKKIM
18	TRIPURA

7.4 Registrar On-boarding Guide & Implementation Support Documents

In order to support the above process and policies, the following implementation support documents have been framed and provided by UIDAI:

Sl.No.	List of Documents
1	Enrolment Planning Template to estimate infrastructure requirements
2	Registrar Readiness Checklist and Readiness Checklist for EA
3	State- Wise List of Empanelled Enrollment Agencies & Model RFP/Q template
4	Enrolment Centre Setup Checklist
5	Resident Enrolment Process Document version 2.2
6	Roles and Responsibility Documents for Verifier/Introducer/Operator/Supervisor/EA/Registrar
7	J4 Device Certification Process (STQC) – Ver 1.1.1.pdf
8	Training & Certification Plan for EA personnel
9	List of Training Agencies & Testing centers
10	Information Security Guidelines for Registrars – July 2011 Edition
11	Data Protection and Security Guidelines
12	Document Management System - process and guidelines
13	Information, Education & Communication Guidelines
14	Financial Inclusion – Solution Overview
15	CSO Outreach – Plan for reaching marginalized segments

7.5 Roles & Responsibilities

To ensure timely readiness to begin enrolments & enforce adequate quality during the enrolment process, the Registrar needs to identify individuals who will carry out the roles outlined below. The detailed responsibilities for each role are listed below:

7.5.1 Responsibilities of Senior Management (Implementation Committee)

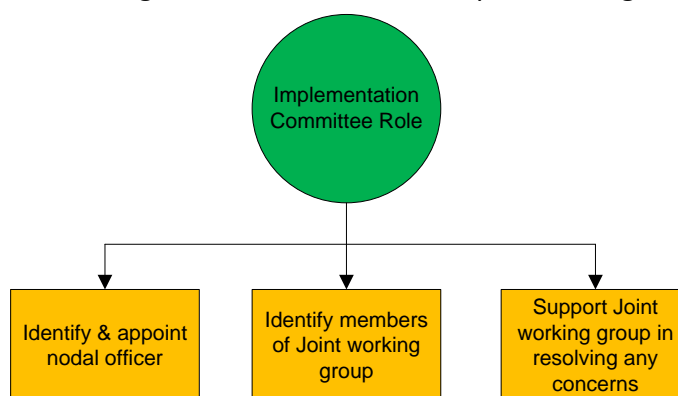The responsibilities of Senior Management can be summed up in the diagram below:

Figure 20: Implementation Committee's role

7.5.2 Responsibilities of Nodal Officers

The responsibilities of Nodal Officers include:

- Ensure a Working Group comprising members from UIDAI & Registrar organization is set up. The committee should have representative from Technology, Process, & IEC (Information, Communication & Education) domains from both organizations.
- Ensure smooth functioning & active participation of the Working Group during UIDAI-Registrar alignment.
- Ensure MOU is signed.
- Ensure Technology, Process & IEC aspects between the two organizations are aligned.
- Advise UIDAI's focal point on modalities for setting up the On-Boarding workshop & attend the same. Ensure required stakeholders & members of Working Group attend the workshop.
- Provide inputs on current practices followed by the Registrar.
- Share Registrar's expectations on AADHAAR usage (number usage, authentication usage, financial inclusion usage etc.) with UIDAI.
- Check if Registrar needs access to biometric data; if required, provide public key to enable access to encrypted data.
- Hire enrolment agencies & share their details with UIDAI.
- Identify & train an Admin person from EA who can carry out ongoing registration of operators, supervisors & enrolment stations.
- Identify supervisors from the Registrar organization who can carry out the verification procedures, monitor the resident enrolment exercise, audit processes followed by EAs & provide the required supervision.
- Ensure supervisors & EA operators are trained & certified.
- Initiate biometric device procurement either via EA or another mechanism deemed right by the Registrar.
- Identify the officer, whom the Contact Centre may forward grievances & share contact details of, with UIDAI.
- Identify authorized Introducers & share details in prescribed template with UIDAI.
- Schedule camps for enrolling & educating Introducers.
- Monitor performance of Introducers & EAs on an on-going basis.
- Develop & Share detailed enrolment plan and schedule with UIDAI.

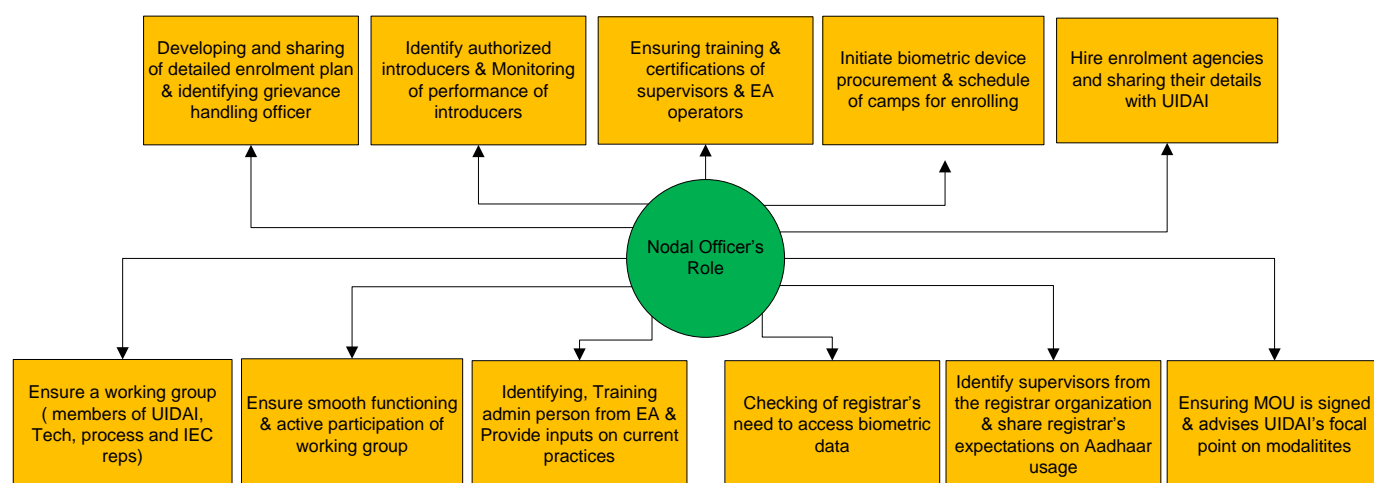The responsibilities of Nodal Officers can be summed up in the diagram below:

Figure 21: Role of Nodal Officers

7.5.3 Responsibilities of Joint Working Group Members

Attend Registrar on-boarding workshops.
- Ensure integration of resident communication plan & material.
- Ensure integration of enrolment & other required processes.
- Ensure integration of KYR+ Software with UIDAI's enrolment client.
- Ensure deliverables / project plan activities as mentioned in the Registrar- UIDAI Readiness Checklist/ Integration Project Plan are executed.
- Define the required communication channel, Issue resolution/Escalation mechanism etc.
- Identify any issues or concerns& suggest appropriate resolution mechanism.
- Develop probable queries/grievances that can come from beneficiaries & correct responses for them.

The responsibilities of Joint Working Group Members can be summed up in the diagram below:

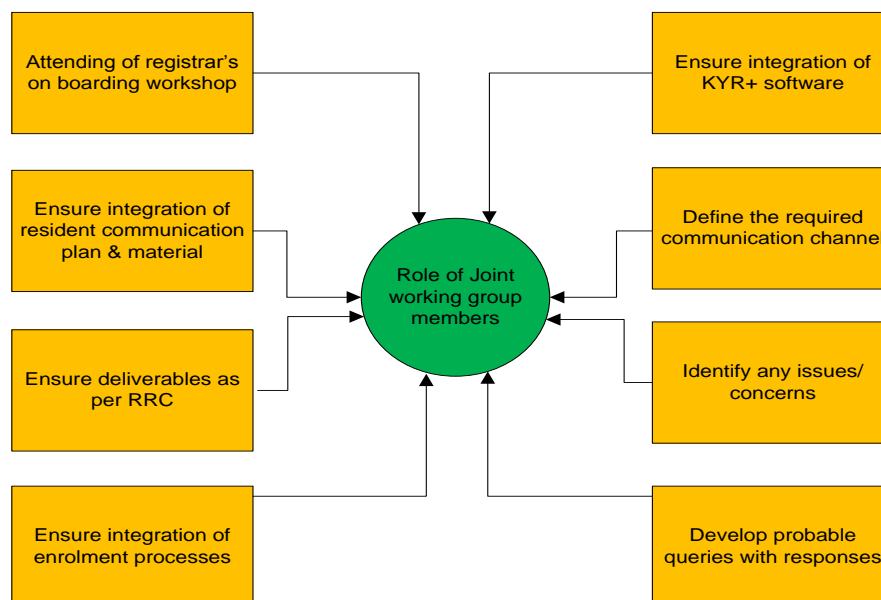**Figure 22: Role of Joint working group members**

7.5.4 Responsibilities of Registrar's Supervisors

The responsibilities of Registrar's Supervisor's include:

- Audit of Enrolment Centers' readiness.
- Audit of enrolment agency processes and their effectiveness.
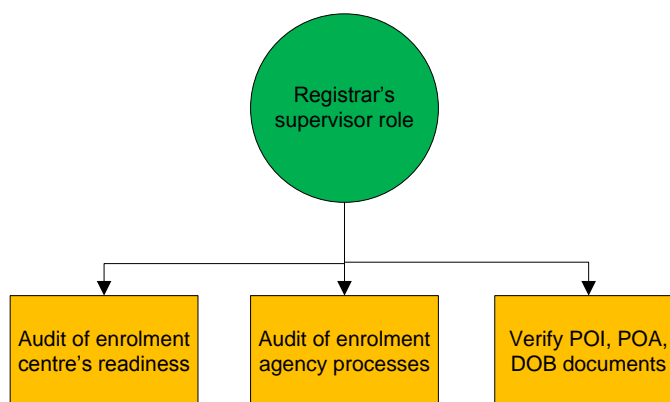- Verify PoI, PoA, DOB documents in case of document based verification as per defined guidelines.

Figure 23: Registrar's supervisor role

7.6   Aadhaar & Civil Society Outreach

It is part of the UIDAI mandate to make special efforts to enable the inclusion of marginalized communities (e.g. the homeless, migrant workers, nomadic/denotified tribes, street children, etc.) in AADHAAR. **The Registrars will be required to evolve and implement a special campaign to cover this target group.** Registrars could also partner with CSOs at the local level to assist them in spreading awareness of AADHAAR among marginalized groups, in planning special enrolment drives for specific groups, and to authorize CSOs as Introducers for those without Proof of Identity and Address.

7.7   Legal Framework

The Unique Identification Authority of India has been set up as an attached office of the Planning Commission. The National Identification Authority of India Bill, 2010 proposes to establish the National Identification Authority of India, thereby giving it the status of a statutory authority established by an Act of Parliament.
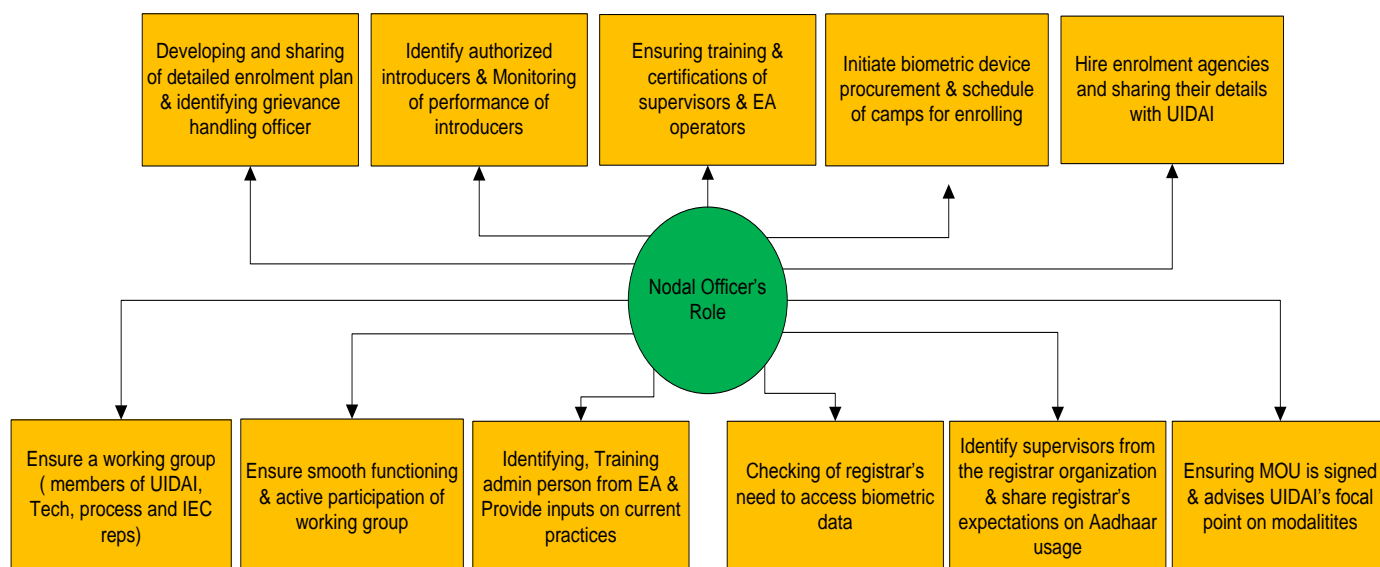

Figure 24: Features of National Identification Authority of India Bill, 2012

Salient features of the National Identification Authority of India Bill, 2010

1. The National Identification Authority of India Bill, 2010, *inter alia*, seeks to provide—
    i. for issue of Aadhaar numbers to every resident by the Authority on providing his demographic information and biometric information to it in such manner as may be specified by regulations;
    ii. for authentication of the Aadhaar number of an Aadhaar number holder in relation to his biometric information and demographic information subject to such conditions and on payment of such fees as may be specified by regulations;
    iii. For establishment of the National Identification Authority of India consisting of a Chairperson and two part-time Members.
2. The Bill has extra territorial application if the act or conduct constituting the offence or contravention involves the Central Identities Data Repository (CIDR).
3. Residents have been defined to mean individuals usually residing in a village or rural area or town or ward or demarcated area (demarcated by the Registrar General of Citizen Registration) within a ward in a town or urban area in India.
4. The Aadhaar number will be a random number and once issued will not be re-assigned. It will not bear any attributes or identity data relating to the Aadhaar number holder.
5. An Aadhaar number, subject to authentication, shall be accepted as proof of identity of the Aadhaar number holder.
6. The response to authentication would be a yes or no only. No demographic information or biometric information will be given as a response.
7. Aadhaar number or the authentication thereof shall not, by itself, confer any right of or be proof of citizenship or domicile in respect of an Aadhaar number holder.
8. The Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health.
9. The Authority shall take special measures to issue Aadhaar number to women, children, senior citizens, persons with disability, migrant, unskilled and un-organized workers, nomadic tribes and such other categories of individuals as may be specified by regulations.
10. The Authority has been cast with an obligation to ensure the security and confidentiality of identity information of individuals. The Authority shall take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorized access or use or unauthorized disclosure.
11. The Authority will be bound to disclose the information in pursuance of an order of the competent Court or in the interest of national security.

12. An Aadhaar number holder shall be entitled to obtain details of request for authentication of his Aadhaar number and the response provided on the request by the Authority in the manner as may be specified by regulations.

13. The Bill provides for the powers which can be exercised by the Authority and also certain functions which can be discharged by it. These, *inter alia*, include—

    i. Specifying the demographic information and biometric information for enrolment for an Aadhaar number and the processes for collection and verification thereof.

    ii. Collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations.

    iii. Appointing of one or more entities to operate the Central Identities Data Repository;

    iv. Maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations.

    v. Specify the usage and applicability of the Aadhaar number for delivery of various benefits and services as may be provided by regulations.

    vi. Setting up facilitation centers and grievance redressal mechanisms for redressal of grievances of the residents, Registrars, enrolling agencies and other service providers.

    vii. Enter into Memorandum of Understanding or agreements with Central Government, State Government or Union Territories or other agencies for the purpose of performing any of the functions in relations to collecting, storing, securing or processing of information or performing authentication.

14. The Bill also provides for offences and penalties for contravention of the provisions of the legislation. Penalties have been, *inter alia*, specified for-

    i. Impersonation at the time of enrolment by providing any false demographic information or biometric information.

    ii. Impersonating or attempting to impersonate another person with the intention of causing harm or mischief to an Aadhaar number holder or with the intention of appropriating the identity of Aadhaar number holder by changing or attempting to change any demographic information or biometric information.

    iii. Unauthorized collection of identity information.

    iv. Disclosing identity information collected in the course of enrollment or authentication to any unauthorized person.

    v. Unauthorized access to the Central Identity Data Repository (CIDR), which also includes –

        • Unauthorized downloading, copying or extracting of data from CIDR,

        • Introducing any virus or other computer contaminant in the CIDR,

        • Damaging the data in CIDR, disrupting the access to CIDR,

        • Denying or causing denial to access the CIDR,

        • Destroying, deleting or altering any information stored in any removable storage media or CIDR,

- Stealing, concealing, destroying or altering any computer source code used by the Authority with an intention to cause damage.

vi.   Tampering with data in CIDR or in any removable storage medium with the intent of modifying information relating to Aadhaar number holder or discovering any information thereof.

vii.   Attempting to give false biometric information for getting an Aadhaar number or updating the information.

7.8   List of Documents for Verifying PoI (Proof of Identity)

Support POI (Proof of Identity) Documents containing Name and Photo

Sl. No.	List of Documents
1	Passport
2	PAN Card
3	Ration/PDS Photo Card
4	Voter ID
5	Driving License
6	Government Photo ID Cards
7	NREGA Job Card
8	Photo ID issued by Recognized Educational Institution
9	Arms License
10	Photo bank ATM Card
11	Photo Credit Card
12	Pensioner Photo Card
13	Freedom Fighter Photo Card
14	Kissan Photo Passbook
15	CGHS/ECHS Photo Card
16	Address Card having Name and Photo issued by Department of Posts
17	Certificate of Identity having photo issued by Group A Gazetted Officer on letterhead
18	Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations

7.9   List of Documents for PoA (Proof of Acceptance)

Supported POA (Proof of Address) Documents containing Name and Address

Sl.No.	List of Documents
1	Passport
2	Bank Statement/Passbook
3	Post Office Account Statement/Passbook
4	Ration Card

Sl.No.	List of Documents
5	Voter ID
6	Driving License
7	Government Photo ID Cards
8	Electricity Bill(not older than 3 months)
9	Water bill(not older than 3 months)
10	Telephone Landline Bill(not older than 3 months)
11	Property Tax receipt(not older than 3 months)
12	Credit Card Statement(not older than 3 months)
13	Insurance Policy
14	Signed Letter having Photo from Bank on letterhead
15	Signed Letter having photo issued by Recognized Educational Instruction on letterhead
16	Signed Letter having Photo issued by registered Company on letterhead
17	NREGA Job Card
18	Arms License
19	Pensioner Card
20	Freedom Fighter Card
21	Kissan Passbook
22	CGHS/ECHS Card
23	Certificate of Address having photo issued by MP or MLA or Group A Gazetted Officer on letterhead
24	Certificate of Address issued by Village Panchayat head or its equivalent authority(for rural areas)
25	Income Tax Assessment Order
26	Vehicle Registration Certificate
27	Registered Sale/Lease/Rent Agreement
28	Address Card having Photo issued by Department of Posts, caste and Domicile Certificate having Photo issued by State Govt.
29	Caste and Domicile Certificate having Photo issued by State Govt.
30	Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
31	Gas Connection Bill (not older than 3 months)
32	Passport of Spouse
33	Passport of Parents(in case of Minor)

7.10   List of Documents for DoB (Date of Birth)

Supported Proof of DOB (Date of Birth) Documents

Sl.No.	List of Documents
1	Birth Certificate
2	SSLC Book/Certificate
3	Passport
4	Certificate of Date of Birth issued by Group A Gazetted Officer on Letterhead

7.11 Technology Overview

The UIDAI will provide enrolment software which will interface with the biometric devices like camera, fingerprints and iris scanners.   The client software will check for image quality and has validations built to ensure demographic and biometric data capture adheres to defined standards.   The software has flexibility to integrate with Registrar applications for pre-enrolment data and KYR+ fields.   An overview of the Enrolment Client flow is given below for reference:
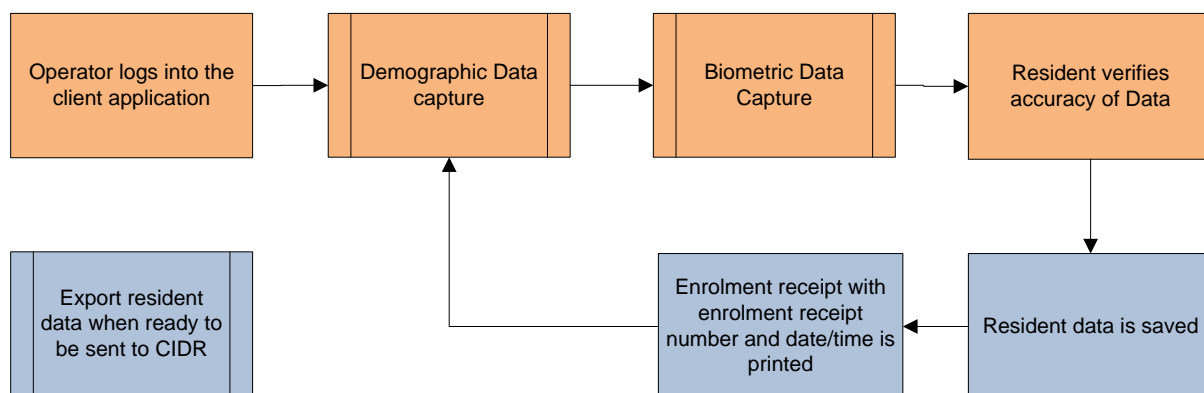

Figure 25: Enrolment Client Process Flow for issuing Aadhaar Numbers

Key features of the software:

- User Authentication
  - Role based user authentication and authorization
  - Application specific login. Users must be pre-registered with CIDR
- Pre-Enrolment Support
  - Capability to upload pre-existing electronic demographic data to enrolment client
- Demographic data capture & Pincode to Region Code mapping
  - Textual data entry of the resident based on supportive documents like Proof of Identification/Address (POI/POA)
  - Supports client with master data file to enable correct mapping from pincode to state, district & Village/Town/City
- Basic Transliteration
  - Conversion of demographic data from English to any Indian official language supported; Language to be converted into is selected as a process of client configuration
- Biometric data capture & quality check

- Integration with biometric devices to capture photograph, IRIS and fingerprint; Vendor neutral quality check to meet quality criteria
- Enrolment Receipt
  - Provide resident an enrolment receipt with an enrolment number, date/time & details of data capture
  - Enrolment receipt number along with date/time can be used for status check of Aadhaar number allocation & track Aadhaar letter once dispatched by India Post
- Secure data storage and data upload
  - Tamper proof transfer of data from enrolment client to CIDR
  - Encryption of data written to offline device using UIDAI public key
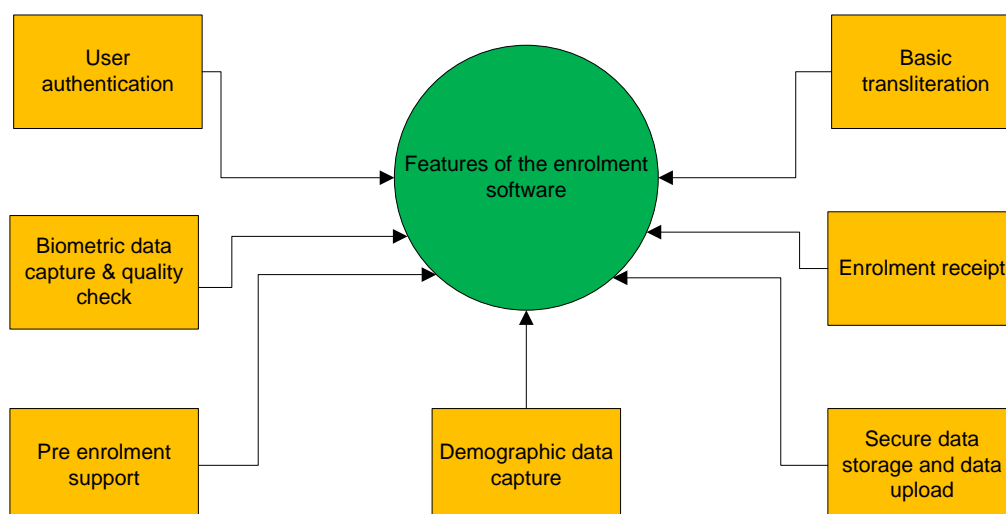 - Auto delete of enrolment data at client through online communication with CIDR

Figure 26: Features for enrolment software

7.12 Pre-enrolment data and KYR+ data Integration

Since the capture of biometrics using sophisticated biometric devices could be the bottle-neck in the entire enrolment process, it is desirable to complete the demographic data capture and verification ahead of the biometric capture. This step is called pre-enrolment. It is possible to use existing databases available to the registrar (For example, state governments BPL, PDS, or NREGA databases) to import demographic data into Aadhaar enrolment client before enrolment. Note that, even with pre-enrolment, final data verification is done at the time of enrolment along with biometric data capture. The data can be imported into Aadhaar enrolment client by loading the pre-enrolment data into a file in a predefined format and then loading the file into enrolment client.

The Aadhaar enrolment client collects basic demographic fields called as KYR (Know Your Resident) data. The registrars may need to capture additional fields called as KYR+ data. For example, PDS might need to capture information such as APL (Above poverty line), BPL (Below poverty line), family details, etc as part of KYR+ data. Aadhaar enrolment client provides a loosely coupled way to integrate KYR data into registrar's software. At the end of every enrolment, Aadhaar enrolment client writes a file containing KYR fields along with a unique enrolment ID into a pre-defined directory. Registrar's software can load this file to capture KYR data and continue to collect additional KYR+ fields.

7.13 Training of Various Stakeholders

UIDAI has a detailed strategy for making training available for all the stakeholders. To achieve efficient training, UIDAI has developed complete training content with assistance of subject matter experts from Project Management Unit (PMU), Technology Team and other senior officials at UIDAI.
For more on training, visit: http://uidai.gov.in/training.html

In order to conduct certification & testing, two testing agencies are employed and testing is done for following roles:

    a) Enrolment Operator
    b) Enrolment supervisor
    c) Enrolment Agency Tech support
    d) Master Trainer

For more on testing & certification, visit:
http://uidai.gov.in/testing-a-certification-portal.html

The two testing agencies are:

    a) Sify Testing & Certification Portal (For more on Sify Testing, refer http://uidai.sifyitest.com/)
    b) Merit Trac Testing & Certification Portal (And more on Merit Trac Testing, refer http://119.226.214.34/UIDAI/)

7.14 Training Overview

Details of Training modules & their duration (in days)

Module Name & course Duration	Master Trainer	Enrolment Operator	Supervisor	Technical Support	Registrar Representatives
UIDAI Overview	0.5	0.5	0.5	0.5	
Introduction to UIDAI enrolment process	0.5	1	1	0.5	1
Basics on Hardware devices (Biometric, camera, PC etc)	0.5	0.5	0.5	0.5	0.5
Working with the bio metric devices	0.5	1	1	0.5	
UID Client Application Software	1.5	2	2	2	0.5
Trouble Shooting on UID Client Application Software and Biometric devices	0.5	0.5	0.5	1	
Setting up an Enrolment center	0.5	---	1	1.5	
Enrolment Centre Management	0.5	---	0.5	0.5	0.5
Exception Handling	0.5	1	1	0.5	
Soft Skills - Interaction with Residents / Senior Residents, Grievance handling,, Crowd handling etc	1	1.5	1.5	0.5	0.5
Training Delivery Techniques	1.5	---	---	---	
Total	**8**	**8**	**9.5**	**8**	**3**

7.15 Information, Education and Communication

Information, Education and Communication (IEC) is an important process in developing and executing the communication strategy for the enrolment and Aadhaar enabled services. The main communication objectives of the UIDAI are as follows:

1. Complete Coverage: Ensure communication reaches each resident of India.
2. Understanding Aadhaar: Ensure all residents understand what Aadhaar is, what benefits it can provide to people and how it will be used going ahead.
3. Understanding the Aadhaar process: Ensure residents understand Aadhaar enrolment process, how and when they can get their Aadhaar and know the grievance handling mechanism.
4. Uniform Understanding: Ensure the above understanding is uniform across residents.
5. Sustain Demand: Reassure the first few experiences on usage of Aadhaar and amplify on positive experiences to further create and sustain demand on a regular basis.

The Registrar, along with the UIDAI Regional Offices and Headquarters are required to disseminate information regarding Aadhaar so that benefits of governmental and other schemes reach the intended beneficiaries.

To ensure comprehensive coverage across all the residents, the message of Aadhaar shall be spread through the following communication channels:

- Broadcast & Telecast: TV, radio, print, internet
- Information: News and publications
- Outdoors: Posters, handouts, wall paintings, banners, hoardings
- Entertainment: Cinema, sports, endorsements
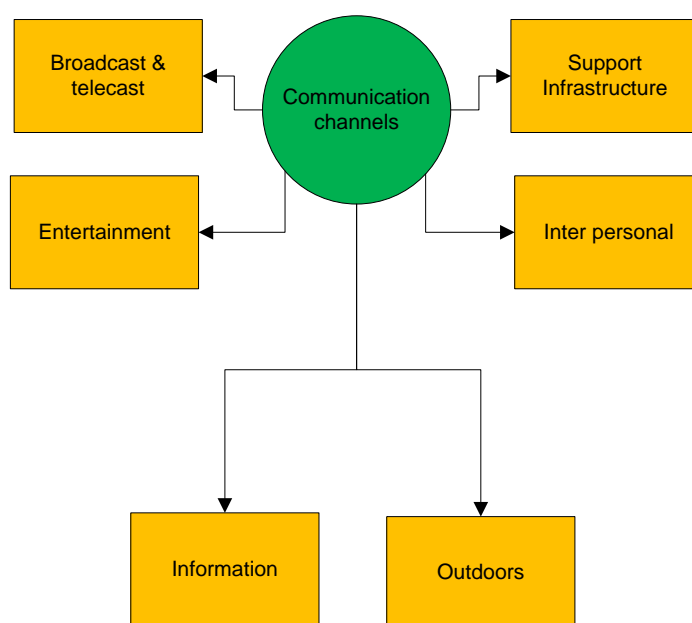- Inter-personal: Audio/video screening, telecom, folk and traditional media

Figure 27: Communication channels

Before undertaking the production and dissemination of creative elements the UIDAI ROs in collaboration with the Registrars prepare IEC plans to be implemented. UIDAI provides all the support and guidance to the Registrars for the activities pertaining to core messaging of Aadhaar - its features and benefits.