Chapter 3 Enrolment, Update and Authentication Ecosystem

3.1 Enrolment and Update Ecosystem

Every resident in the country is eligible to obtain an Aadhaar number by submitting his/her demographic and biometric information. After verification of this information by UIDAI Aadhaar numbers are issued. UIDAI confirms the uniqueness of the identity of a resident by way of a de-duplication process where the information submitted by each new enrollee is matched with that of others in the Aadhaar database to ensure that the applicant is not already enrolled. After establishing uniqueness of identity, a 12-digit random number is generated and issued to the applicant. This unique lifetime number cannot be assigned to any other individual. The demographic and biometric details of Aadhaar holders, however, can be updated to ensure continued accuracy of the information in the CIDR.

An Aadhaar number subject to its authentication[11], is accepted as a valid proof of identity of the Aadhaar number holder for receiving specified benefits, subsidies and services for which expenditure is met from the Consolidated Fund of India/Consolidated Fund of State. However, Aadhaar does not confer citizenship or domicile to its holder and is only a proof of identity.

The definition of “Resident” gains prime importance as it sets the basic eligibility criteria for entitlement of Aadhaar number. A “Resident”, as per the Act, is as an individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment.

The enrolment process begins with a resident submitting his/her demographic and biometric information to the Enrolment Agency (EA) along with prescribed supporting documents to establish identity, date of birth and address of the enrollee. The information is submitted to the CIDR for further processing and generation of Aadhaar number. The UIDAI has adopted a tiered model consisting of Registrars and EAs for enrolment and updation of Aadhaar numbers. The information to be provided at the time of enrolment are as follows:

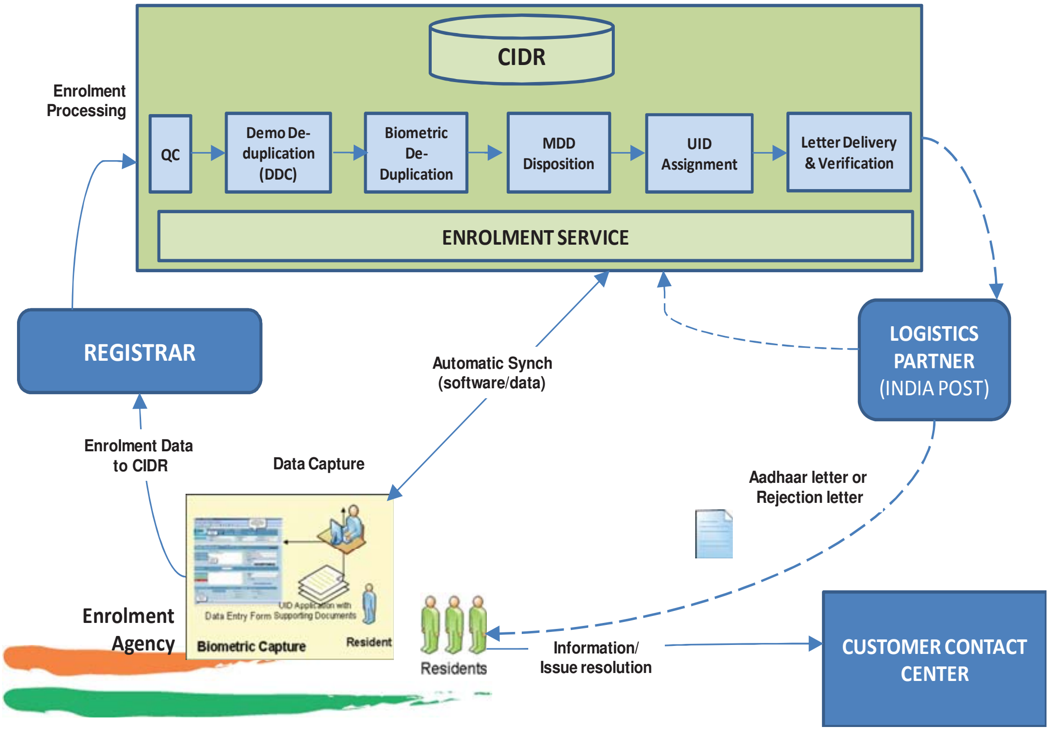
Demographic information	Name, verified date of birth or declared age, gender, address, mobile number (optional) and email ID (optional), in case of introducer-based enrolment- introducer name and introducer’s Aadhaar number, in case of Head of Family based enrolment- name of Head of Family, relationship and Head of Family’s Aadhaar number; in case of enrolment of child- enrolment ID or Aadhaar number of any one parent, proof of relationship (PoR) document.
Biometric information	Ten fingerprints, two iris scans, and facial photograph

[11] Authentication is the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository of UIDAI for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

Aadhaar enrolment (and mandatory biometric updates) is done free of cost for residents. However, for all enrolments and mandatory biometric updates, UIDAI makes payments to the Registrars at rates fixed by them from time to time[12].

The enrolment process is illustrated in **Figure 3.1**.

Figure 3.1 Enrolment process


CIDR
Enrolment Processing
QC
Demo De-duplication (DDC)
Biometric De-Duplication
MDD Disposition
UID Assignment
Letter Delivery & Verification
ENROLMENT SERVICE
REGISTRAR
Automatic Synch (software/data)
LOGISTICS PARTNER (INDIA POST)
Enrolment Data to CIDR
Data Capture
Aadhaar letter or Rejection letter
UID Application with Data Entry Form Supporting Documents
Enrolment Agency
Biometric Capture
Resident
Residents
Information/ Issue resolution
CUSTOMER CONTACT CENTER

Graphics Courtesy: UIDAI

3.1.1 Key Regulations and Amendments

Enrolment and Update is central to the Aadhaar structure. Registrars and EAs, responsible for collecting the demographic and biometric information of individuals for the enrolment process, are core components of this ecosystem. EAs are responsible for adherence to processes prescribed by UIDAI and to ensure data quality. The Aadhaar (Enrolment & Update) Regulations 2016 and amendments thereto govern the activities associated with this ecosystem. Key regulations and amendments thereto governing the Aadhaar enrolment and update process are given in **Table 3.1**.

Being the backbone of the Aadhaar system, it is important that the regulations prescribe the processes and procedures in conformity with the provisions of the Aadhaar Act and UIDAI establish systems to ensure that Aadhaar numbers generated satisfy all the features and qualities envisaged in the Act.

[12] Effective from January 2019, the rate for every enrolment that has resulted in successful generation of an Aadhaar number is fixed at ₹100. Similarly, for all mandatory biometric updates UIDAI pays ₹100 per request to the Registrar with effect from January 2019. However, for all voluntary updates of demographic or biometric information, UIDAI has prescribed a fee of ₹50 per request (enhanced to ₹100 per request for voluntary biometric updates w.e.f. 09 May 2020) and is to be paid by the Aadhaar number holder.

Table 3.1: Key Regulations and amendments thereto governing the Aadhaar Enrolment and Update ecosystem

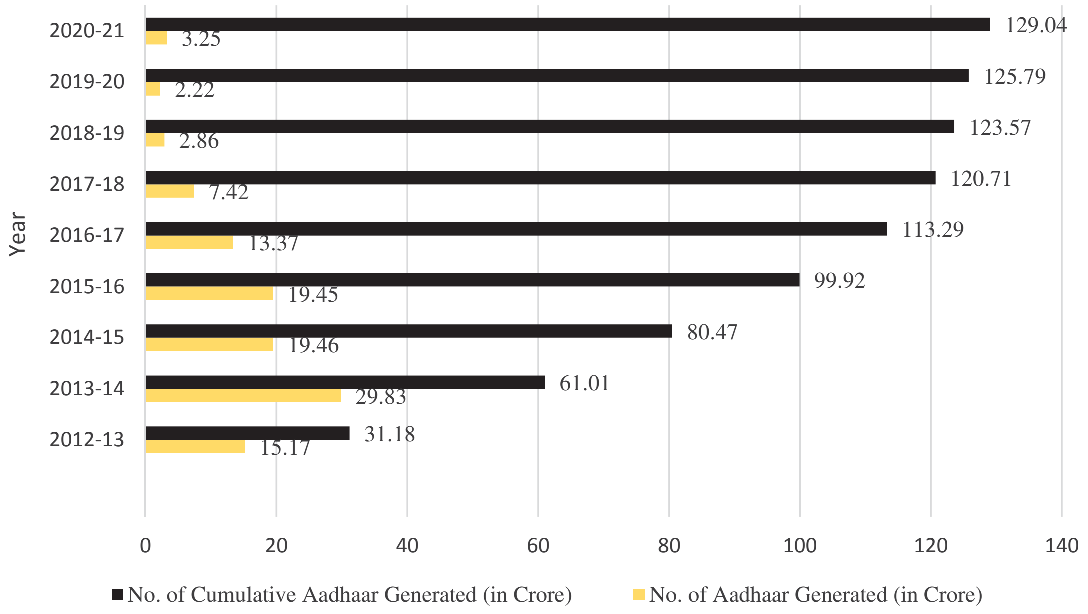
Key Regulations	Key features
Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) Dated 14-Sep-2016	✓ Resident Enrolment Process: Biometric & Demographic information required, Role of Registrars, Collection of Information, Equipment, Software used in enrolment etc. ✓ Generation, Rejection & Delivery of Aadhaar numbers. ✓ Update of Resident information: Mandatory update, Modes of update, Convenience Fee to be charged for update ✓ Appointment of Registrars, Enrolling Agencies & other service providers ✓ Omission or Deactivation of Aadhaar number ✓ Grievance Redressal Mechanism. ✓ Format of enrolment/ Correction & update form, list of Documents (POI, POA, POR, DOB etc.), Code of conduct for Service providers
Aadhaar (E&U)) (Second Amendment) Regulations 2017 (No. 2 of 2017) Dated 07-Jul-2017	✓ Addition of Regulation 12A: Any Central or State department or agency requiring authentication or possession of Aadhaar for receipt of any subsidy, benefit or services should ensure enrolment of such individual who is yet to be enrolled or update their Aadhaar details, by setting up enrolment centres at their premises
Aadhaar (E&U)) (Fourth Amendment) Regulations 2017 (No. 5 of 2017) Dated 31-Jul-2017	✓ Immediate suspension of activities or imposition of Financial Disincentives on Registrar or Enrolment Agency or any service provider or any other person or Cancellation of the credential, codes or permission issued to them, for violation of any regulation, process, standard, guideline or order, by a Registrar or Enrolment Agency or any service provider or any other person
Aadhaar (E&U)) (Sixth Amendment) Regulations 2018. (No. 2 of 2018) Dated 31-Jul-2018	✓ New Definition of Incapacitated Person. ✓ Date of Birth of resident can be updated only once. In case the DoB is to be updated more than once, it can only be done through an exception handling process which may require the resident to visit the Regional Office (RO) of the UIDAI. ✓ Amendments in verification of update data, disclosure of information to parents/ form to be signed by parents in case of minors. ✓ Introduction of Aadhaar Address update PIN Service for residents not having acceptable proof of Address.

Aadhaar (E&U)) (Seventh Amendment) Regulations 2019. (No. 3 of 2019) Dated 05-Sep-2019	✓ Enhancement in list of POI, POA, POR & DOB under Schedule II of E&U Regulations, 2016 [Regulation 10(2)]

3.1.2 Status of Aadhaar Enrolment and Update

UIDAI had generated 129.04 Crore Aadhaar numbers as of March 2021 for the residents in the country, which is approximately 94 *per cent* of the projected population. The number of Aadhaar generated and updated during 2012-13 to 2020-21 are given in **Chart 3.1** and **Chart 3.2** respectively.

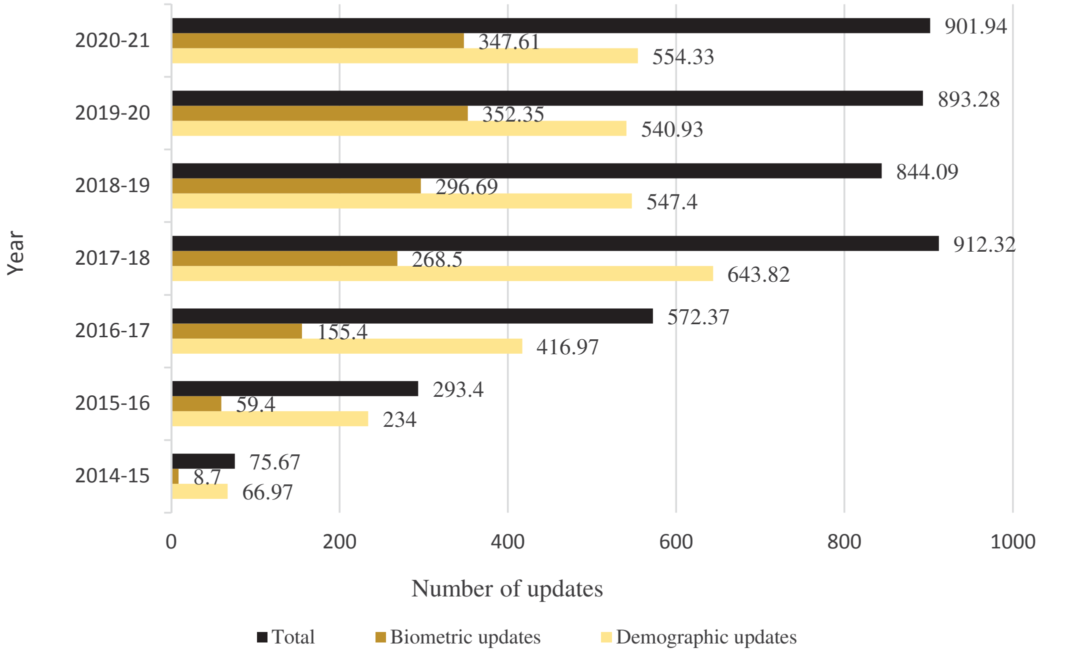
Chart 3.1: Generation of Aadhaar (in Crore)



(Data Source: UIDAI)

Chart 3.1 shows that growth of Aadhaar generated in 2013-14 was 95.67 *per cent* as compared to previous year and gradually it reached the plateau after 2017-18 wherein it grew less than 3 *per cent* as compared to previous year.

Chart 3.2: Aadhaar Update (in Lakh)



(Data Source: UIDAI)

Chart 3.2 shows that growth of Aadhaar update had picked up pace from 2015-16 onwards. The total updates at the end of 2014-15 standing at 75.67 Lakh has multiplied around 12 times in five years to reach at 901.94 Lakh at the end of 2020-21.

3.1.3 Aadhaar Saturation Status

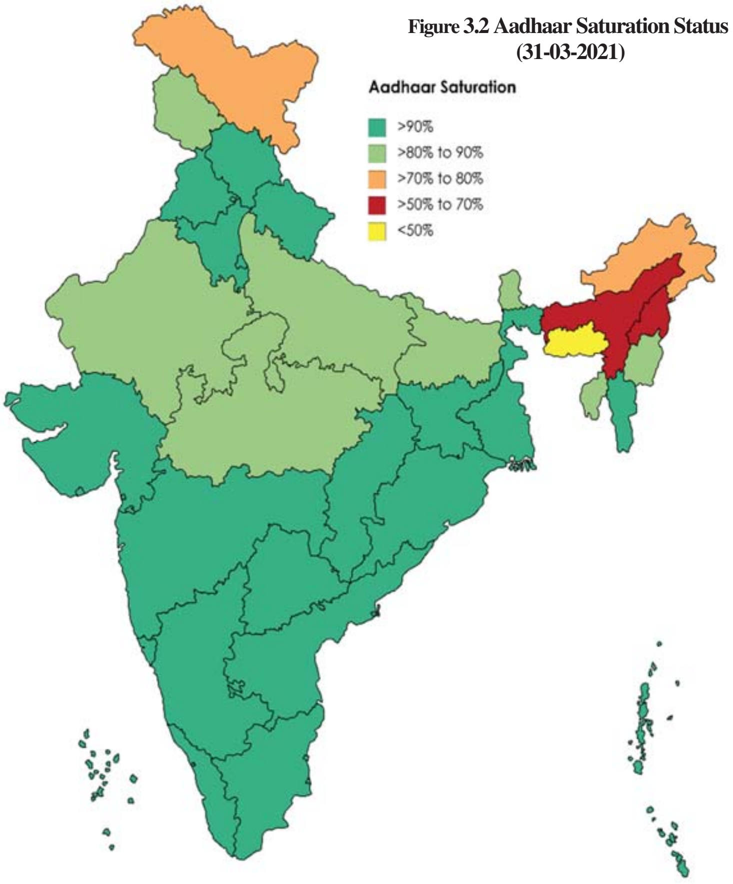


Figure 3.2 Aadhaar Saturation Status (31-03-2021)

Figure 3.2 depicts the Aadhaar saturation status across the States and Union Territories as on 31 March 2021. UIDAI had issued more than 124.67 Crore (live) Aadhaar till 31 March 2021[13] and in 23 States/ Union Territories more than 90 *per cent* saturation levels were achieved whereas *eight* States/ Union Territories had saturation of around 80 to 90 *per cent*. In two States/ Union Territories (Arunachal Pradesh and Ladakh) the saturation level is between 70 to 80 *per cent* whereas in other two States (Assam and Nagaland) the saturation status was above 50 *per cent* but less than 70 *per cent*. However, one State (Meghalaya) has not reached the saturation level of 50 *per cent*. There was overall saturation of 91 *per cent* in issue of Aadhaar across India.

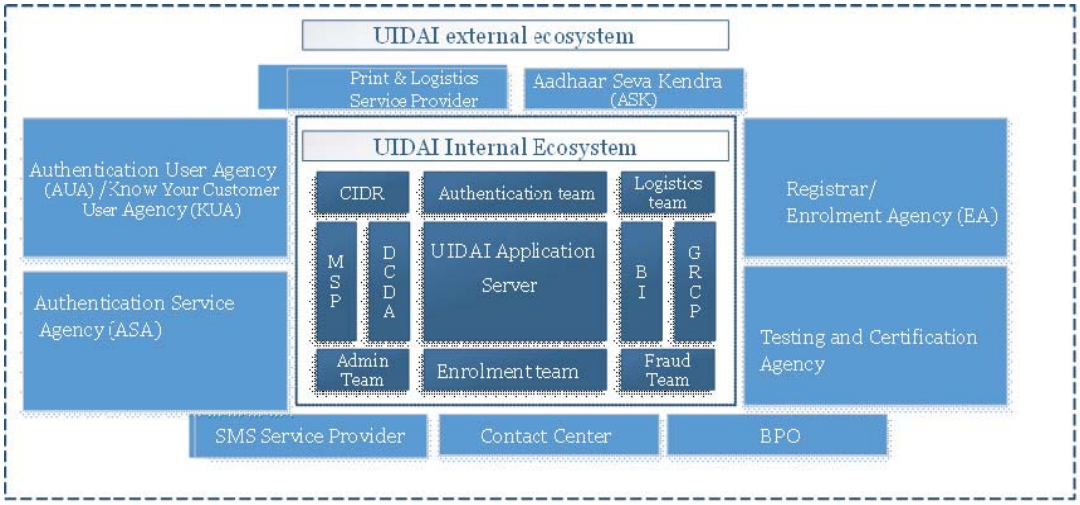
Thus, the UIDAI needed to continue with its efforts to enroll Aadhaar eligible residents and increase the enrolment in States which have not achieved 90 *per cent* benchmark.

3.1.4 The Components of Aadhaar Ecosystem

The various components of the ecosystem, external as well as internal, involved in the enrolment to authentication, printing to delivery of Aadhaar card and the customer support is depicted in the **Figure 3.3**.

[13] Source: Aadhaar Saturation Report of UIDAI as on 31 March 2021.

Figure 3.3: The Aadhaar Ecosystem


UIDAI external ecosystem
Print & Logistics Service Provider
Aadhaar Seva Kendra (ASK)
Authentication User Agency (AUA) /Know Your Customer User Agency (KUA)
Authentication Service Agency (ASA)
UIDAI Internal Ecosystem
CIDR
Authentication team
Logistics team
M S P
D C D A
UIDAI Application Server
B I
G R C P
Admin Team
Enrolment team
Fraud Team
Registrar/ Enrolment Agency (EA)
Testing and Certification Agency
SMS Service Provider
Contact Center
BPO

3.1.5 De-duplication process

UIDAI has employed a two-step process for identifying duplicate enrolments. In the first stage, demographic data match is done and in the second stage biometric matching of fingerprints and iris with the database of all others enrolled in the Aadhaar database is done to identify duplicates and establish uniqueness of the enrollee. After successful clearance at the de-duplication stage, a 12-digit Aadhaar number is generated which is communicated to the resident through UIDAI's logistics partner India Post. Residents who have submitted their mobile numbers during enrolment can also download e-Aadhaar[14].

UIDAI has agreements with three vendors for providing Automatic Biometric Identification Systems (ABIS). These vendors were selected by the Managed Service Provider (MSP). If one ABIS identifies a duplicate, it will be subject to verification by another ABIS for enhancing accuracy. Further, UIDAI has a manual adjudication system also where duplicates identified are subject to a further verification before rejection. UIDAI also undertakes demographic de-duplication to identify errors in the demographic data submitted by a resident at the time of enrolment.

Details of de-duplication carried out by UIDAI as on 31 March 2019 are given below:

A. Biometric Residents

Aadhaar generated through Biometric De-duplication through

(i) ABIS: 111,11,40,041

(ii) Manual De-duplication: 89,45,010

B. Non-Biometric Residents:

Aadhaar generated without Biometric

(i) Children below five years: 11,48,27,267

[14] An e-Aadhaar is an electronic form of Aadhaar letter downloadable from e-Aadhaar portal of UIDAI's website. Resident can download e-Aadhaar in pdf format by visiting https://eaadhaar.uidai.gov.in . They can use either 28-digit enrolment no. received at the time of enrolment or 12-digit Aadhaar Number.

(ii) Residents with 100 *per cent* Biometric exception category: 5,69,196

Issues of large member of de-duplications done and Aadhaar issued to minor children are commented in Report.

3.1.6 Bio-metric Device Certification

Standardization, Testing and Quality Certification (STQC) Directorate, an attached office of MeitY, is the nodal agency appointed to carry out specifications as well as certification activity for enrolment and authentication devices requirements for the UIDAI.

3.1.7 Managed Service Provider

The entire end-to-end technology infrastructure of UIDAI including data center operations, management of IT systems of UIDAI ROs, technical helpdesk etc., is managed by the Managed Service Provider (MSP) viz M/s HCL Infosystems Ltd. The MSP was appointed in August 2012 through Expression of Interest and Request for Proposal method for a period of seven years. At present (March 2021), the MSP is functioning under extension period. The total value of contract with the MSP was ₹1,978.62 Crore.

3.1.8 Governance Risk Compliance and Performance – Service Provider

Government Risk Compliance and Performance – Service Provider (GRCP-SP) is an independent monitoring agency on behalf of UIDAI, deployed by the Authority to ensure compliance and security of the UIDAI ecosystem. The role of GRCP-SP is to facilitate creation of a robust, comprehensive, secure environment for UIDAI to operate. (including external agencies such as a Registrars, Enrolment Agencies, Aadhaar Seva Kendra's, ASAs, AUA/ KUA/ Sub-KUAs, Contact Center, SMS Service Provider and Logistics Service Providers etc.), in terms of Visibility, Effectiveness and Control.

Service level monitoring of all contracts is one of the important works of the GRCP-SP, which helps the UIDAI in having a financial control. All the data pertaining payments is to subjected to GRCP Audit and processed for payments on the basis of their reports.

3.2 Audit Observations on Aadhaar Enrolment Ecosystem

Audit observations on the Aadhaar Enrolment *vis-à-vis* provisions of the Aadhaar Act 2016 are given in succeeding paragraphs:

3.2.1 Verification of the 'Resident' status of the applicants

UIDAI relied on self-declaration made by the residents regarding their 'Resident' status at the time of Aadhaar enrolments and thus status of Resident or non-Resident remained unverified.

As per the provisions of the Aadhaar Act, 2016, every resident in the country is entitled to obtain an Aadhaar number by submitting his demographic and biometric information by undergoing the process of enrolment. A "Resident" as per the Act, is as an individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment. The definition of "**Resident**" sets the basic eligibility criteria to be fulfilled by each individual for obtaining Aadhaar.

The Aadhaar (Enrolment and Update) Regulations 2016 prescribes the nature of documents a resident should submit as proof of identity (PoI), proof of address (PoA), date of birth (DoB), proof of relationship (PoR) etc. to the EAs. Whenever a resident applies for enrolment/ correction/ updation, a standard form containing demographic details of self along with ticking the residential status, has to be filled

It was however, noted that UIDAI had not specified any proof/document in the regulation for confirming the "Resident" condition, to qualify as a resident. No procedure has been prescribed to check the veracity of the applicant's testimony. Thus UIDAI had not put in place a system for fulfilling the fundamental requirement of identifying residents. Audit is of the view that non-verification of status of residence may lead to issue of Aadhaar to non-bona fide residents.

UIDAI stated (September 2019) that the validity of the documents provided by individual applicants in support of identity, address, date of birth etc., are confirmed during enrolment and cases appearing as fraudulent are dealt in accordance with provisions of Aadhaar (Enrolment & Update) Regulations 2016. UIDAI (October 2020) asserted that self-declaration in conjunction with the prescribed documents was the only practical means to ascertain the resident status of applicants. The Ministry of Electronics and Information Technology (MeitY) agreed (June 2021) with replies of UIDAI to the audit observations.

The replies of UIDAI/ MeitY are not tenable as Aadhaar (Enrolment & Update) Regulations 2016 stipulates actions to be taken against fraudulent cases only after generation of Aadhaar numbers, whereas the issue here is of conducting prior checks to ascertain residential status of an applicant, as one of the condition for issue of Aadhaar, as provided in the Aadhaar Act 2016. UIDAI should explore a workable system of verification of residence status based on the criteria prescribed under the Act. A review of the definition of a resident for this purpose has gained more importance in light of the fact that non-resident Indians holding a valid Indian passport were also entitled for an Aadhaar number after their arrival in India bypassing the 182 days residency criteria as per the Gazette notification dated 20 September 2019.

Recommendation: ***UIDAI may prescribe a procedure and required documentation other than self-declaration, in order to confirm and authenticate the residence status of applicants in line with the provisions of the Aadhaar Act.***

3.2.2 Generation of Multiple Aadhaar

De-duplication process remained vulnerable for generating multiple Aadhaar numbers and manual interventions had to be done to resolve the problem.

De-duplication process ensures that the Aadhaar numbers generated are unique and no second number is assigned to the same resident by comparing the resident's demographic and biometric information collected during the process of enrolment, with the records in the UIDAI database. It also ensures that a data with an already assigned Aadhaar number cannot be used to generate a new number to another resident.

As per information provided by UIDAI Tech Centre, nearly 4.75 Lakh duplicate Aadhaar numbers were cancelled as of November 2019. This data indicated that on an average no less than 145 Aadhaars generated in a day during the period of nine years since 2010 were duplicate numbers requiring cancellation.

Besides this, verification of records at the UIDAI Regional Office Bengaluru showed that residents reported 5,388[15] cases of issue of multiple Aadhaars during the period 2015-16 to 2019-20 forcing UIDAI to cancel the second Aadhaar issued, based on complaints received. We could not ascertain the number of multiple Aadhaars reported at other ROs as access to the related documents was not given to us. UIDAI HQ also could not provide RO wise data on the number of multiple Aadhaars and stated (September 2019) that such data was not available with them. Apart from issue of multiple Aadhaars to the same resident, instances of issue of Aadhaars with the same biometric data to different residents were also seen reported in RO Bengaluru.

Further, information like the date of issue of first Aadhaar, the date of issue of subsequent Aadhaars and the time taken to identify and cancel them were also not provided to Audit limiting our scope for further scrutiny on the issue.

UIDAI stated (September 2019) that the biometric de-duplication ensures uniqueness with accuracy of 99.9 *per cent,* but in cases where residents with poor biometrics enroll, their accuracy could be slightly poor which could lead to generation of multiple Aadhaars. It was also informed that UIDAI has deployed self-cleaning system (an automated process) to identify duplicate Aadhaars and for taking corrective actions. However, no details on the frequency of the deployment of the self- cleaning system, the number of duplicates detected through the process etc., were provided to audit as of July 2020. The fact that residents reported 860 cases of multiple Aadhaars in Bengaluru RO alone during 2018-19 suggested that the self- cleaning system employed by UIDAI was not effective enough in detecting the leakages and plugging them. Though the number of cases reported could be termed as miniscule when compared with the total number of Aadhaars generated.

UIDAI later, (October 2020) explained the "whitelisting process" invoked in case a genuine person is denied Aadhaar through the de-duplication process. It claimed significant improvements in detecting duplicate and fraudulent enrollment after application of Service Level Agreement (SLA) parameters independently for each of the three Biometric Service Providers (BSPs) and incorporation of other SLA parameters like FNIRA[16], attack presentation classification error rate etc. in the new contract. UIDAI also informed that a project with IIIT Hyderabad in the field of biometric was going on to develop indigenous technology to achieve "atmanirbharta". MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

It is evident that UIDAI was aware of generation of multiple Aadhaar which had remained unidentified/detected by it unless brought to their notice. It was also noted that to ensure provision of unique identities to residents, UIDAI has even resorted to Manual De-duplication (MDD) processes in cases where biometric data was rejected by BSPs. The cancellation of duplicate Aadhaars or generation of Aadhaars through MDD indicated flaws in the functioning of BSPs appointed by UIDAI. The failure in De-duplication resulting in denial of Aadhaar can be negated by invoking the whitelisting process for the aggrieved residents. As a result, UIDAI/MeitY needs to devise foolproof mechanisms for capturing unique biometric data.

[15] The total 5,388 cases of multiple Aadhaar reported comprises of 1,131, 2,339, 330, 860 & 728 cases during the years 2015-16, 2016-17, 2017-18, 2018-19 & 2019-20 respectively.

[16] FNIRA: False Negative Identification Rate for Anomalous matches

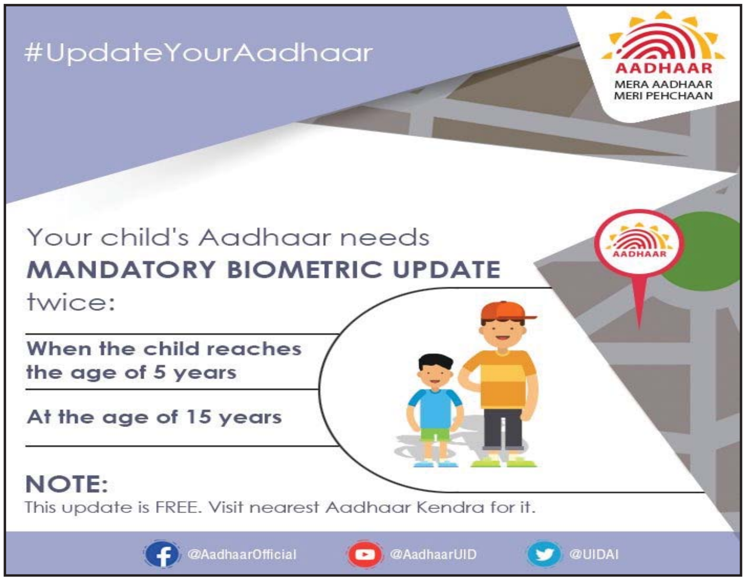
UIDAI also needs to strengthen the Automated Biometric Identification System so that generation of multiple Aadhaars can be curbed at the initial stage itself.

Recommendation: ***UIDAI may tighten the SLA parameters of Biometric Service Providers (BSPs), devise foolproof mechanisms for capturing unique biometric data and improve upon their monitoring systems to proactively identify and take action to minimize, multiple/duplicate Aadhaar numbers generated. UIDAI may also review a regular updation of technology. UIDAI also needs to strengthen the Automated Biometric Identification System so that generation of multiple/duplicate Aadhaars can be curbed at the initial stage itself.***

3.2.3 Enrolment for Aadhaar of Minor Children below age of five years

The uniqueness of identity, one of the distinctive attributes of Aadhaar, was not ensured while issuing Aadhaar to minor children below the age of five years.

As per the provisions of the Aadhaar Act, 2016, every resident in the country is entitled to obtain an Aadhaar number by submitting his demographic and biometric information by as part of the enrolment process. However, as per Aadhaar (Enrolment and Update) Regulations 2016, biometrics are not captured for Aadhaar generation in respect of minor children below five years of age. Their UID is processed as per Section 5 (1) of these Regulations on the basis of demographic information and facial photograph by linking with the UID of any one of the parents. These children are required subsequently, to update their biometrics (ten fingers, iris and facial photograph), when they turn five and then again on attaining fifteen years of age.



#UpdateYourAadhaar

AADHAAR
MERA AADHAAR
MERI PEHCHAAN

Your child's Aadhaar needs
MANDATORY BIOMETRIC UPDATE
twice:

When the child reaches the age of 5 years

At the age of 15 years

NOTE:
This update is FREE. Visit nearest Aadhaar Kendra for it.

@AadhaarOfficial @AadhaarUID @UIDAI

(Image courtesy: UIDAI)

UIDAI regulations state that if a child having attained the age of five or fifteen years of age, fails to update his/ her biometric information within two years of attaining such age, his/ her Aadhaar number would be deactivated. In cases where such update had not been carried out at the expiry of one year after deactivation the Aadhaar number would be omitted.

Further, UIDAI notified (September 2018) that if the current age of an Aadhaar holder enrolled as a child had crossed 15 years and if his/ her biometrics are not updated such Aadhaar would be cancelled.

Audit observed that since UIDAI does not capture biometrics of minor children below five years for generating Aadhaar, the basic condition for issue of Aadhaar i.e. uniqueness of identity was not being met. As per information furnished, UIDAI had generated approximately

11.48 Crore Aadhaars for children below five years till March 2019. The assistance provided to the Registrars/ Enrolment agencies for enrolment @ ₹27 per child along with related costs worked out to ₹310 Crore.

UIDAI informed, that they had deactivated about 40.91 Lakh Aadhaar for want of Biometric Update as on 01 November 2019. With the increase in saturation level, there remains always a possibility that children whose Aadhaar has been deactivated as mentioned above might have enrolled themselves afresh after crossing the age of five, with their biometrics.

Gift your child a unique identity
Even Infants can be enrolled for Aadhaar
Know More

(Image courtesy: UIDAI)

Based on the Hon'ble Supreme Court's judgment[17], that no subsidy, benefits, or services could be denied to a child to whom no Aadhaar number was assigned, we are of the view that, the issue of cards, devoid of biometric authentications to children below five years served limited purpose considering the costs involved.

UIDAI stated (June 2020) that it is mandated to issue Aadhaar number to all the residents, including children. Even though, biometrics of children are not collected, child Aadhaar is issued based on authentication of a parent. It added that the chances of creation of duplicate Aadhaar were very low even in the absence of biometric data, and the number of duplicate numbers found/ reported was insignificant. They claimed that issuing an identity to a child, led to monetary savings for the exchequer as it helped eliminate ineligible beneficiaries, and was hence beneficial. They were of the view that the cost incurred was insignificant.

In its subsequent reply (October 2020), UIDAI accepted that the de-duplication done based on the demographic data and photograph may not be as robust as the automated biometric identification system (ABIS). They issue SMS and letters to all the parents/ guardians whose children were due for mandatory update for bringing them back in the Aadhaar ecosystem. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

We are of the view that the UIDAI's mandate was to issue Aadhaar number to a resident after establishing uniqueness of the applicant through his/her biometrics. Therefore, issue of Aadhaar numbers to children without biometric data did not meet the criteria of establishing the uniqueness of the holder and could not be justified on the grounds of the mandate to issue ID to all residents including children. Moreover, as per judgment of the Supreme Court on

[17] Five bench Supreme Court Judgement dated 26 September 2018 on writ petition (civil) No. 494 of 2012 & connected matters

Aadhar, no subsidy, benefits or services cannot be denied to a child for want of an Aadhar number.

Issue of Bal Aadhar to minor children below five years, without capturing their unique identity could not be justified on basis of unquantified advantages as suggested by UIDAI. The fact that an individual is required to apply for regular Aadhar cards for at two stages after crossing five years, UIDAI requires to review the issue of non- mandatory Aadhar to minor children below five years. They may explore alternate ways to capture unique identity of minor children below five years, in keeping with its mandate.

Recommendation: ***UIDAI may explore alternate ways to capture uniqueness of biometric identity for minor children below five years since uniqueness of identity is the most distinctive feature of Aadhaar established through biometrics of the individual.***

3.2.4 Management of Aadhaar Documents

All the Aadhaar numbers stored in the UIDAI database were not supported with documents on the demographic information of the resident, causing doubts about the correctness and completeness of resident's data collected and stored by UIDAI prior to 2016.

Upto July 2016, it was the responsibility of the Aadhaar Document Management System (ADMS) (M/s Hewlett Packard Sales India Private Ltd. (HP)) to store the physical sets of records provided by individuals at the time of enrolment, both in electronic as well as physical form in a secured manner. The documents[18] collected by the Enrolment Agencies (EAs) during enrolment/ update were picked up by the ADMS agency on a regular basis from EAs for scanning and uploading into a portal. With effect from July 2016, UIDAI mandated inline scanning[19] of residents' documents[20] bringing an end to pick-up of the documents by the ADMS Agency in June 2017.

As significant gaps were noted in the enrolments done and documents submitted by the Registrars/EAs to the DMS Agency, UIDAI issued (December 2015) a set of instructions with the aim of minimizing the gaps and to reconstruct missing documents, for compliance by the DMS agency, the Tech Centre, ROs and Registrars/ EAs. Accordingly, the Tech Centre was to compare the list of Enrolment Identity (EID[21]) received from the DMS agency and generate State/ Registrar/ EA wise list of such EIDs against which Aadhaar has been generated but data prepared by the Agency was missing. The Registrars were to forward the information received from Tech Centre to its EAs for collection of missing documents. The ROs in their turn, were to guide the Registrars/ EAs for reconstruction of data and monitor this activity. The ROs were to furnish monthly progress report (State/ Registrar/ EA wise) to UIDAI HQ showing the number of EIDs requiring reconstruction, number of EIDs for which reconstruction completed and the number of EIDs for which reconstruction was not completed.

[18] Enrolment Identification Documents collected from the residents as their proof of identification, proof of address, proof of date of birth or relationship etc., along with the copy of enrolment/ update form.

[19] Inline scanning is the process where the original documents are scanned and uploaded with the enrolment/ update form to the CIDR at the time of enrolment/ update itself and hence no physical copy is retained/ collected by the operators.

[20] Proof of identification, proof of address, proof of date of birth or relationship etc.

[21] EID- means a 28-digit Enrolment Identification Number allocated to residents at the time of enrolment.

These instructions further suggested that not all the Aadhaar numbers stored in the UIDAI database were supported with documents on the demographic information of the resident, raising questions on the correctness and completeness of resident's data collected and stored by UIDAI.

Data on the number of EIDs against which Aadhaar has been generated but documents were missing and the nature of document(s) identified as missing along with the status of their reconstruction was sought from UIDAI. UIDAI informed (June 2020) that the MSP (Managed Service Provider) had been given the responsibility to map EID-UID linkage for which software development was under progress. It was also informed that with effect from 01 July 2016, inline scanning and upload of Personally Identifiable Information (PII) documents along with enrolment and update packets have been made mandatory and hence all new Aadhaar numbers generated and updated after 01 July 2016 are presumed to have their PII documents. It was further added that since update of Aadhaar numbers by residents is a regular activity, the reconstruction of PII documents was a continuous process and the documents collected from Registrars and EAs were being uploaded/ reconciled, the exact position of deficiency of PII documents had not been worked out.

The response of UIDAI suggested that the enrolments were carried out without confirming availability of all required documents. UIDAI, despite being aware of the fact that not all Aadhaar numbers were paired with the personal information of their holders, was yet to identify the exact extent of mismatch though nearly ten years have elapsed since the issue of first Aadhaar. Non pairing of biometric data in the system with demographic information was not in consonance with the instructions issued by UIDAI and non availability of PII documents with the Authority, for those already collected from the residents, impacts the reliability of the Aadhaar database. Further, any quality check of demographic data by UIDAI post issue of Aadhaar will lead to deactivation of these Aadhaar numbers as stipulated by the Regulations. As a matter of fact, till 01 November 2019, 37,551 Aadhaar numbers were deactivated due to disputed PII documents.

Therefore, UIDAI may identify and fill the missing documents by taking proactive steps at the earliest in order to avoid any legal complications or inconvenience to Aadhaar holder due to suspension/ deactivation of Aadhaar for want of paired PII documents.

UIDAI agreed (October 2020) with the audit recommendation and assured to explore the possibility to fill the gaps in documentation without causing avoidable inconvenience to Aadhaar holders. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

Recommendation: ***UIDAI may take proactive steps to identify and fill the missing documents in their database at the earliest, in order to avoid any legal complications or inconvenience to holders of Aadhaar issued prior to 2016.***

3.3 Audit Observations on Aadhaar Update Ecosystem

Audit observations on the Aadhaar Update Ecosystem is given below:

3.3.1 Voluntary Biometric Updates

High numbers of voluntary biometric updates indicated deficient capture of biometric during enrolments resulting in Authentication failures resulting in residents having to update their biometrics.

Biometric updates fall into two categories viz., mandatory updates and voluntary updates.

A. Mandatory updates usually arise in the following situations:

- **a.** A child with age less than five years at the time of initial enrolment should provide biometric information on attaining the age of five years and this initial capture is treated as a mandatory update of an existing Aadhaar.
- **b.** Children aged between five and 15 years at the time of enrolment should furnish all biometrics for updates when turns 15 years.

B. Voluntary updates may arise in following situations:

- **a.** Age more than 15 years at the time of enrolment – Residents are recommended to update their biometric data every ten years.
- **b.** Events like accidents or diseases leading to biometric exception
- **c.** Biometric updates arising out of authentication failures (False Rejects – where authentication attempts of a resident with valid Aadhaar number is rejected) resulting from incorrect biometric capture or poor biometric quality captured at the time of enrolment.

While mandatory updates are free for the residents, voluntary updates are chargeable for the residents at rates prescribed by UIDAI.

An analysis of data on biometric updates for the year 2018-19 revealed that during the year, UIDAI updated 3.04 Crore biometrics data successfully. Out of the successful updates, 0.81 Crore (26.55 *per cent*) were mandatory and the remaining 2.23 Crore (73.45 *per cent*) were voluntary updates.

According to UIDAI, the need for biometric update could arise on account of authentication failures (called "false rejects"- where a correct resident with a valid Aadhaar Number is incorrectly rejected) due to incorrect biometric capture or poor biometric quality captured at the time of enrollment. Thus, a significantly high percentage of voluntary biometric updates indicated occurrence of a high volume of authentication failures, which compel Aadhaar number holders to update their biometrics. This was also a reflection on the quality of biometric data stored in CIDR for establishing the uniqueness of the Aadhaar number holder. It was observed that the UIDAI takes no responsibility for deficient biometric capture and the onus of updating biometric is passed on to the Aadhaar number holders and they are also required to pay for such updates.

UIDAI stated (July 2020) that it was not possible to ascertain reasons for authentication failures or attribute it to incorrect/poor quality biometrics at the backend. It however, confirmed that biometric mismatch could happen due to reasons such as poor quality of biometric capture at the time of enrollment, improper placement of finger at the time of authentication, entering of incorrect Aadhaar number and device quality issues. UIDAI also stated that as per the approved procedure for enrollment, operators could complete the enrollment even with poor quality biometrics through "forced capture" after four unsuccessful attempts to capture biometric data. It was reported that this procedure was adopted to improve inclusiveness of residents under the Aadhaar programme.

UIDAI agreed (October 2020) with audit observations and explained that most authentication was based on fingerprints which do change in adults with time based on their job profiles. Further, the two other modes of authentication viz "Iris" and "Face" could also be utilized but the devices for Iris checks were comparatively more expensive than the fingerprint authentication devices and efforts were on to introduce more technically certified devices for Iris checks. It also added that it was requesting their ecosystem partners to deploy Iris authentication devices. UIDAI had also developed a model for face authentication which was under trial phase, and that it planned to utilize all the three modes of authentication to overcome the lacunae faced in fingerprint authentications. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

While noting the action taken/ proposed by UIDAI to improve upon the capture of biometrics, we are of the view that acceptance of poor-quality biometrics at the time of enrolment showed that UIDAI had not ensured the quality of biometric data included in the CIDR, adversely impacting the programme's objective of establishing the uniqueness of the Aadhaar number holder. Further, acceptance of poor-quality biometrics on the plea of expanding the enrollment under the programme and then passing the burden of the updation of biometrics cost to Aadhaar holders did not seem appropriate. Since UIDAI is not in a position to identify reasons for authentication failures of biometrics, it is felt that charging residents a fee for voluntary update of their biometrics was not in order, for no fault of them.

Recommendation: ***UIDAI may review charging of fees for voluntary update of residents' biometrics, since they (UIDAI) were not in a position to identify reasons for biometric failures and residents were not at fault for capture of poor quality of biometrics.***

3.4 Aadhaar Authentication Ecosystem

Entities engaged in providing Aadhaar enabled services can avail the authentication services of UIDAI. The authentication facility allows verification of the identity information of an Aadhaar number holder by providing a Yes/ No response or e-KYC data.

Authentication services are provided online and in real-time basis through its Data centers and are offered through the following modes:

a. **Demographic authentication**: Aadhaar number and demographic data submitted for authentication is matched with the corresponding data in the CIDR.

b. **One Time Pin (OTP) based authentication**: OTP is sent to the mobile number or e-mail address of the Aadhaar holder registered with the Authority and the Aadhaar number and OTP is matched with the OTP sent by UIDAI.

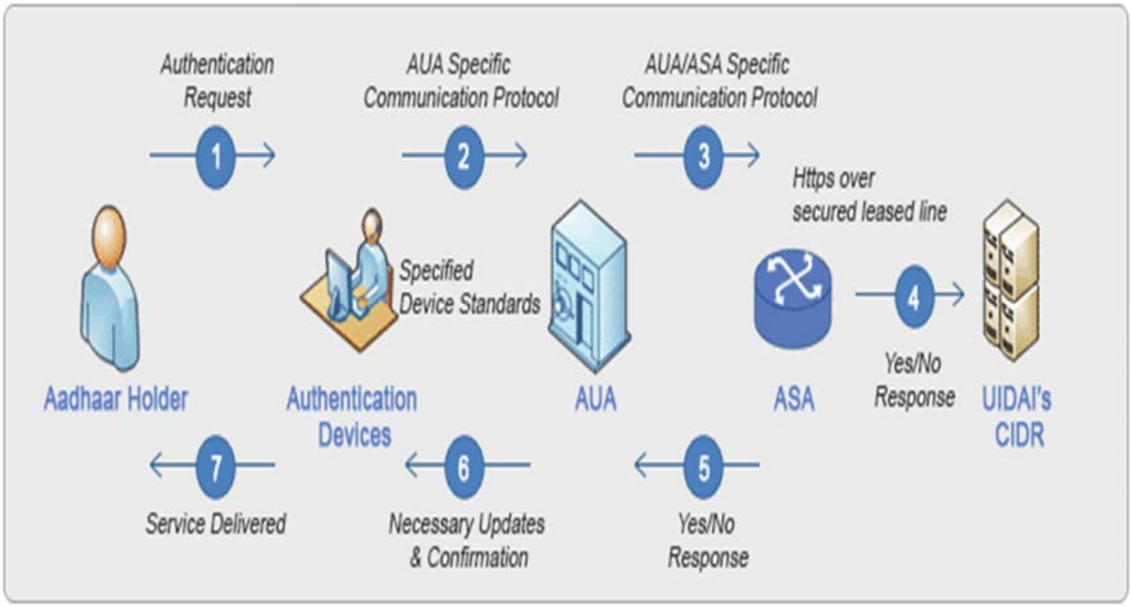
c. **Biometric based authentication**: The Aadhaar number and biometric information submitted by the Aadhaar holder is matched against the biometric data of said Aadhaar number stored in CIDR.

d. **Multi-factor authentication**: A combination of two or more of the above modes.

3.4.1 Aadhaar Authentication partners

The main players in authentication eco-system are the Authentication User Agencies[22] (AUAs)/ e-KYC User Agency[23] (KUA) or the Requesting Entity (RE)[24] and the Authentication Service Agencies[25] (ASAs). A requesting entity submits the Aadhaar number and demographic information or biometric information of an individual through an ASA, to the CIDR for authentication. The ASA provides the infrastructure for connectivity and related services for enabling a requesting entity to undertake authentication. There were 164 AUAs, 162 KUAs and 22 ASAs entities active as on 31 March 2021. The Aadhaar authentication process is illustrated in **Figure 3.4**.

Figure 3.4: Aadhaar Authentication Process


Authentication Request
1
AUA Specific Communication Protocol
2
AUA/ASA Specific Communication Protocol
3
Https over secured leased line
Specified Device Standards
4
Yes/No Response
Aadhaar Holder
Authentication Devices
AUA
ASA
UIDAI's CIDR
7
6
5
Service Delivered
Necessary Updates & Confirmation
Yes/No Response

(Image courtesy: UIDAI)

3.4.2 Key Regulations and Amendments

Key regulations relating to Aadhaar authentication are given in **Table 3.2**.

[22] UIDAI provides Yes/ No authentication services through requesting entities called Authentication User Agency (AUA). AUA is any government/ public legal entity registered in India that uses Aadhaar authentication for providing its services to the residents/customers. An AUA is connected to the UIDAI Data Centre/ Central Identities Data Repository (CIDR) through an ASA.

[23] KUA is a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility.

[24] Requesting Entities are Authentication User Agencies (AUAs) and e-KYC User Agencies (KUAs).

[25] ASA is an agency that has secured leased line connectivity with CIDR. They play the role of enabling intermediaries through secure connection established with the CIDR. ASAs transmit authentication requests of AUAs to the CIDR and transmit back the CIDR's response to the AUAs.

Table 3.2: Key regulations and amendments thereto governing Aadhaar Authentication System

Key Regulations	Key features
Aadhaar (Authentication) Regulations 2016 (No. 03 of 2016) Dated 14-Sep-2016	✓ **Authentication Framework-** Types/ Modes of Authentication, capturing of biometric information, Consent of/ Notification to holder, Devices, Client applications used, Biometric Locking etc. ✓ **Appointment of Requesting Entities & Authentication Service Agencies-** (Procedures, Eligibility Criteria, Roles & Responsibilities, Obligations, Code of Conduct, maintenance of logs, Audit, Data Security, Surrender, Liabilities & Action in case of Default etc.) ✓ **Use of Yes/No & e-KYC authentication** ✓ **Authentication Transaction Data & its Records**- Storage& Maintenance of Transaction Data, Duration of Storage, Access by Aadhaar holder
Aadhaar (Pricing of Aadhaar Authentication Services) Regulation 2019 Dated 06-Mar-2019	✓ Aadhaar Authentication Services to be charged (including taxes) @ ₹20 for each e-KYC transactions and @ ₹0.50 for each Yes/No authentication transaction by requesting entities. ✓ Exemption to Government entities and Department of Posts and conditional exemptions to Scheduled Commercial Banks engaged in Aadhaar enrolment & update facilities

3.4.3 Status of Authentication Transactions

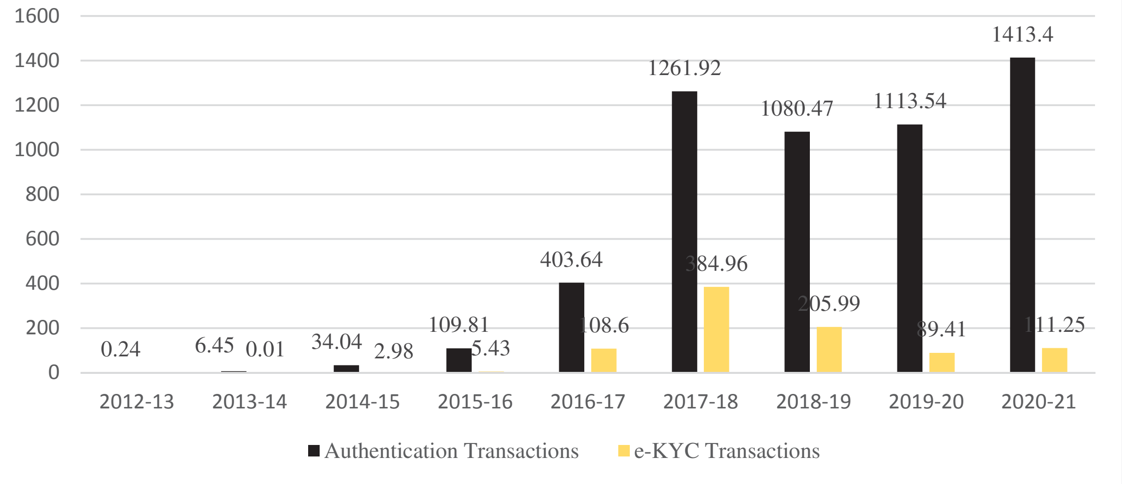
Aadhaar authentication is the process by which the CIDR, based on the information available with it, verifies the correctness of the Aadhaar number submitted to it along with the demographic and biometric information for verification. UIDAI provides two types of authentication services viz. "Yes/ No[26]" authentication facility and "e-KYC[27]" authentication facility using Aadhaar.

As of March 2021, UIDAI has performed more than 5,400 Crore authentication transactions and above 900 Crore e-KYC transactions. The year wise authentication and e-KYC transactions are as in **Chart 3.3**.

[26] "Yes/ No" Authentication: UIDAI started Yes/ No Authentication facility in February 2012 under which requesting entity sends Aadhaar and necessary demographic and/ or OTP and/ or biometric information of the Aadhaar number holder in an encrypted format. UIDAI validates the input parameters against the data stored in CIDR and authenticates in a 'Yes or No' response.

[27] e-KYC Authentication: UIDAI started e-KYC Authentication facility in May 2013 under which a requesting entity sends Aadhaar and necessary biometric information and/ or OTP from the Aadhaar number holder in encrypted format. UIDAI validates the input parameters against the data stored in CIDR therein and returns authentication response as an encrypted digitally signed e-KYC.

Chart 3.3: Authentication and e-KYC Transactions (in Crore)



3.5 Audit observations on Monitoring of Ecosystem partners on compliance to the provisions of Aadhaar (Authentication) Regulations 2016

Aadhaar authentication framework comprises of REs and ASAs. These entities collect the biometric information of the Aadhaar holder for validation purposes. Their interaction with Aadhaar number holders and UIDAI is through the digital mode. Aadhaar (Authentication) Regulation 2016 and other directions of UIDAI notified from time to time, contain instructions on the arrangements which all the entities involved in the authentication ecosystem should follow for ensuring the security of data of the residents. The regulation also specifies the responsibilities of UIDAI in monitoring e-compliance with its instructions by the ecosystem partners' viz. ASA, AUA, KUA etc.

Audit observations on compliance with provisions of the Regulation and the processes put in place by UIDAI to monitor the activities of the REs and ASAs are given in the succeeding paragraphs.

3.5.1 Incidences of Authentication Errors

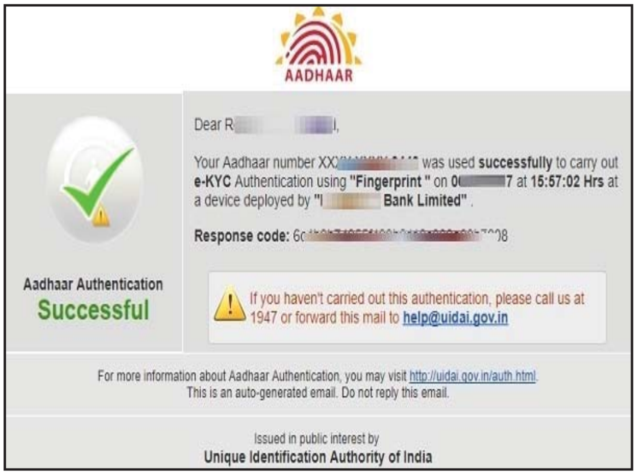
Aadhaar was conceived to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services to Aadhaar number holders by means of successful authentication. The fingerprint authentication transaction success rate remained a cause of dissatisfaction among the users due to biometric authentication failures.

Authentication services of UIDAI is a tool relied upon by government departments to confirm the genuineness of recipients of various benefits from government schemes and programmes. Inaccurate authentication therefore, would lead to errors in identification with consequent implications for effective delivery of services and benefits. In addition, authentication errors compel an Aadhaar number holder to update his/her biometric data. As per a Government of India Report[28] Aadhaar authentication failures in certain States were as high as *49 per cent* in 2016-17.

[28] The Economic Survey 2016-17 (Refer 9.76) published by the Ministry of Finance: "While Aadhaar coverage speed has been exemplary, with over a billion Aadhaar cards being distributed, some states report authentication failures: estimates include 49 *per cent* failure rates for Jharkhand, six *per cent* for Gujarat, five *per cent* for Krishna District in Andhra Pradesh and 37 *per cent* for Rajasthan"

On the subject of authentication errors, UIDAI informed (July 2020) that it does not receive location data during authentication, and in the absence of State-wise information on authentication failures reasons for the same have not been analyzed.

UIDAI further explained (October 2020) that there might be failure of fingerprint authentication in the first attempt due to various reasons, but subsequent attempts may succeed. It claimed that there had been improvement in transaction wise fingerprint authentication success rate from 70-72 *per cent* in 2016-17 to 74-76 *per cent* in 2019-20. It mentioned that to address connectivity issues, buffer authentication had been allowed to REs and in addition, efforts were underway to promote iris authentication and launch face authentication on pilot basis. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.



Dear R[redacted],

Your Aadhaar number XX[redacted] was used **successfully** to carry out **e-KYC** Authentication using **"Fingerprint"** on 0[redacted]7 at **15:57:02 Hrs** at a device deployed by **"I[redacted] Bank Limited"**.

Response code: 6c[redacted]08

Aadhaar Authentication
Successful

If you haven't carried out this authentication, please call us at 1947 or forward this mail to help@uidai.gov.in

For more information about Aadhaar Authentication, you may visit http://uidai.gov.in/auth.html.
This is an auto-generated email. Do not reply this email.

Issued in public interest by
Unique Identification Authority of India

Image 3.1: Illustrative image of authentication success.
Image courtesy: www.basunivesh.com

While there may be various reasons for fingerprint authentication requiring multiple attempts for authentication, this may result in dissatisfaction to Aadhaar holders for repeated biometric authentication failures. The promotion or launch of other forms of biometric authentication might improve the success rate of transactions but their performance has not yet been tested on large scale.

Also Audit has not been provided any basis on which UIDAI has claimed the success rate mentioned here as improvement in failure rates.

Audit is of the view that since Aadhaar as an instrument facilitates good governance through authentication, UIDAI may make efforts to improve the success rate of authentication and also take action to analyze failure cases.

Recommendation: ***UIDAI may make efforts to improve the success rate of authentication transactions by analysing failure cases.***

3.5.2 Non verification of the infrastructure and technical support of Requesting Entities and Authentication Service Agencies

UIDAI did not verify the infrastructure and technological support claimed by the REs and ASAs independently before onboarding the entities in the Aadhaar authentication ecosystem.

The Aadhaar (Authentication) Regulations 2016 stipulate that agencies seeking to become REs and ASAs should fulfill the criteria laid down by UIDAI. Regulation 12 of the Aadhaar (Authentication) Regulation, details the conditions for appointment of REs and ASAs. The regulation authorizes UIDAI to verify the information furnished by the applicants in support of their eligibility through physical verification of documents, infrastructure and technological support, before approval of the applications.

In this context, data on systems put in place for physical verification of the infrastructure and technological support claimed by the applicants for appointment as REs, and details of audit undertaken of infrastructure and technical systems of the REs prior to their appointment were sought (July 2019) from UIDAI. In response UIDAI informed (June 2020) that they had not felt the need so far for conducting physical verification of the infrastructure and technical systems of the applicants prior to signing agreements with them. It was further informed that the REs while moving from pre-production to production environment, were required to submit an IS Audit Report from a CERT-IN empaneled Auditor which was scrutinized by UIDAI.

As of March 2021, 326 REs (164 AUAs and 162 KUAs) and 22 ASAs were active in production environment of the CIDR. Out of these 326 REs, 43 AUAs and 41 KUAs were Government entities whereas out of 22 ASAs, 12 ASAs were Government entities. Further six Government REs (three AUAs & three KUAs) and 44 other than Government REs (22 AUAs & 22 KUAs) had permission in pre-production environment as of March 2021. UIDAI had not verified information furnished by any of the applicants independently (October 2020).

UIDAI accepted (October 2020) the audit observation and assured that it would conduct thorough verification of the documents, infrastructure and technological support before on-boarding the entities (REs and ASAs) in Aadhaar ecosystem. It added that such verification would however, be conducted at the discretion of UIDAI keeping in view the nature of AUA/ KUA and the urgency of implementing authentication service. UIDAI will initiate measures to implement it to the extent possible also keeping in view the constraints posed due to the ongoing Covid- 19 pandemic. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

Therefore, UIDAI should institute a mechanism for physical verification of the documents, infrastructure, and technological support before on-boarding the entities (REs and ASAs) to ensure high standards of IS security across the Aadhaar authentication ecosystem. Audit appreciates UIDAI's decision to conduct physical verification of the documents, infrastructure and technological support before on boarding the entities (REs and ASAs) in Aadhaar ecosystem. However, use of discretionary power to not conduct any verification should be governed by a well-defined criteria/ benchmarks and exemptions from physical verification of the entities, may be granted in exceptional cases only, in interest of IS concerns.

Recommendation: ***UIDAI may conduct thorough verification of the documents, infrastructure, and technological support claimed to be available, before on-boarding the entities (Requesting Entity and Authentication Service Agencies SAs) in the Aadhaar ecosystem.***

3.6 Other related Audit Observations

Audit observations on compliance with provisions of the Regulation and the processes put in place by UIDAI related to the Aadhaar Enrolment, Update and Authentication ecosystem has already been discussed in the foregoing paragraphs. The other important and related observations are discussed in the following paragraphs:

3.6.1 Data Archival Policy

UIDAI is maintaining one of the largest biometric databases in the world; but did not have a data archiving policy, which is considered to be a vital storage management best practice.

Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that remains important to the organization for future reference or regulatory compliance reasons. It is a storage management best practice for efficient use of storage space and performance enhancement. UIDAI is maintaining one of the largest biometric databases in the world and hence it is vital for the Organization to have a policy on archiving the data collected.

It was seen in audit that during the Aadhaar enrolment process, data packets containing demographic and biometric information of the residents are subjected to various processes like Quality Checks (QC), Demographic de-duplication, Biometric de-duplication, Manual de-duplication (MDD) etc., to identify and weed out erroneous/ duplicate/ junk packets. Audit observed that packets rejected at QC stage remained present in the UIDAI database along with the accepted packets. So even where packets are rejected on account of de-duplication, UIDAI apparently will have more than one set of biometric data of the same resident - one with an Aadhaar number attached and others with all details except an Aadhaar number (new enrolment request) and all the data are retained in the CIDR. Retaining any data requires valuable resources, hence valid and necessary data should be only archived. In absence of a data archiving policy, UIDAI retains and preserves large volumes of redundant/ excess data for longer periods.

With a sound data archival policy, an organization like UIDAI, can not only have access to all classes of data whenever the need arises but also reduce the size of storage by disposing off redundant data regularly. It is therefore vital that UIDAI frames a Data Archival Policy and implements it strictly. UIDAI agreed (October 2020) with the audit recommendation and assured to work towards framing a suitable Data Archiving Policy. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Recommendation: ***UIDAI may frame a suitable data archival policy to mitigate the risk of vulnerability to data protection and reduce saturation of valuable data space due to redundant and unwanted data, by continuous weeding out of unwanted data .***

3.6.2 Delivery of Aadhaar Documents

UIDAI did not work out a customized delivery solution with DoP to ensure last mile successful delivery of Aadhaar letters.

Aadhaar cards in laminated form are printed and dispatched by UIDAI in all the cases of successful enrolments and updates. DoP is the logistic partner for delivery of Aadhaar letters as First-Class Mail (Ordinary Post). The ordinary post services of India Post do not provide any individual dispatch number or tracking facility.

As more than 250 welfare schemes of the Government require identification through Aadhaar, possession of Aadhaar assumes importance for residents to avail benefits from these schemes. An effective delivery mechanism is thus vital to ensure that Aadhaar letters are delivered to the intended individuals. Also as per the Aadhaar Act 2016, UIDAI is responsible for the security of the identity information of the Aadhaar holder. In cases of non-receipt of Aadhaar letters by post, an individual can receive the original Aadhaar letter by approaching the Grievance Cell of UIDAI or by downloading e-Aadhaar. UIDAI also introduced an "Order Aadhaar Reprint" (OAR) service in December 2018.

Unique Identification Authority of India
Government of India
AADHAAR
Mera Aadhaar, Meri Pehchaan
Did not get
AADHAAR by Post
or lost it?
ORDER AADHAAR REPRINT
in just a minute, to get updated
copy of Aadhaar via Speed Post
To order a Reprint:
SCAN
or Visit uidai.gov.in
The service is available for a nominal charge of ₹50, including cost of Speed Post.
@AadhaarOfficial
AadhaarUID
@UIDAI
uidai.gov.in
1947 (Toll Free)
help@uidai.gov.in

(Image courtesy: UIDAI)

Audit observed that UIDAI received back 50 Lakh Aadhaar letters at its Bengaluru Centre till March 2019 due to non-delivery to residents. Residents also made complaints about non-delivery of Aadhaar letters at UIDAI Grievance Cell and through RTI requests.

Further, dumping/ abandoning of Aadhaar letters in bulk without delivering to the residents had been highlighted in various news media also.

As UIDAI has availed Ordinary Post Services from DoP, it was not in a position to track the receipt of the physical Aadhaar card by the addressee. In absence of any formal agreement or MoU as regards manner of delivery of Aadhaar letters with India Post, UIDAI had not ensured the confidentiality aspect of Aadhaar cards issued.

UIDAI informed (July 2020) that more than 122 Crore Aadhaar letters have been successfully delivered and DoP is regularly being addressed to ensure and strengthen the delivery of Aadhaar letters.

UIDAI further informed (October 2020) that it has requested DoP to develop a customized tracking system for Aadhaar letters to monitor their delivery and to sensitize their personnel/ staff in ensuring proper delivery to the residents. In addition, UIDAI has facilitated residents with an option to download their 'e-Aadhaar' or use official mobile app 'm-Aadhaar'. Besides, UIDAI started (December 2018) Order Aadhaar Re-print (OAR) Service for residents by using which any Aadhaar holder could order online Aadhaar letter by paying ₹50 per order and get it through Speed Post service of DoP. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

In this regard, Audit noted the action taken by UIDAI but they could have negotiated with India Post for a customized delivery solution for delivery of Aadhaar letters. The options like 'e-Aadhaar', 'm-Aadhaar' and 'OAR' have several limitations requiring the residents to have additional resources and efforts, whereas a doorstep delivery of laminated Aadhaar letters has its own advantage for residents from all walks. Since a large number of Aadhaar cards/ letters were not actually delivered to residents, it raises doubts on the number of Aadhaar cards shown as issued. Thus UIDAI should strengthen its last mile delivery mechanism to ensure effective delivery of the cards issued coupled with security of the identity information.

Recommendation: ***UIDAI may address the delivery problems with their logistic partner namely DoP, by designing a customized delivery model, which will ensure delivery of Aadhaar letters to the correct addressee.***