# Chapter 5 Security of Aadhaar Information System

## 5.1 Introduction

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.

## 5.2 Monitoring of the activities of authentication ecosystem partners of UIDAI

Aadhaar enabled services are provided to the Aadhaar holders through the Authentication User Agencies (AUAs) or the e-KYC User Agencies (KUAs). In addition to AUAs/ KUAs, there are sub-AUAs who use Aadhaar authentication to enable their services through an existing Requesting Entity (RE). The Aadhaar Act 2016, Aadhaar (Authentication) Regulations, 2016, Aadhaar (Data Security) Regulations 2016 and other instructions/ directions issued by UIDAI govern the responsibilities and activities of these entities. Since the authentication facility uses the demographic and biometric information of the Aadhaar holder, it was imperative to put in place a strong and effective monitoring mechanism to ensure that these entities comply with the standards prescribed by UIDAI while operating and maintaining their information systems.

Audit comments on the monitoring of the activities of the authentication ecosystem partners by UIDAI are in the following paragraphs.

### 5.2.1 Annual Information System audit of the operations of REs and ASAs

***UIDAI was neither able to derive required assurance that the entities involved in the authentication ecosystem had maintained their information systems which were compliant with the prescribed standards nor did it ensure compliance of Information Systems Audit by the appointed entities.***

As per UIDAI Regulations on Authentication, REs and ASAs should ensure that their operations and systems are audited by an Information Systems Auditor duly certified by a recognized body, on an annual basis to ensure compliance with UIDAI's standards and specifications. The report of these auditors should be on request, shared with the Authority. Further, the REs will be responsible for the authentication operations of their sub-contractors and would be responsible for ensuring that the authentication related operations of such third-party entities comply with standards and specifications set by UIDAI. The operations of all the entities are to be regularly audited by approved independent audit agencies.

Important Information System (IS) audit requirements are summarized in **Table 5.1**.

**Table 5.1: Information System Audit requirements**

| RE | ASA | UIDAI |
|---|---|---|
| • Ensure audit of its operations and systems by information systems auditor certified by a recognized body on an annual basis.<br>• Share the audit report with the Authority upon request.<br>• Responsible for the authentication operations and results of its sub-contract by third parties.<br>• Ensure the authentication related operations of such third-party entities comply with Authority standards and specifications and they are regularly audited by approved independent audit agencies. | • Ensure that an information systems auditor certified by a recognized body audits its operations annually. | • Audit of the operations, infrastructure, systems and procedures of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they performed authentication, and authentication Service Agencies, either by itself or through audit agencies appointed by it.<br>• The Authority may conduct the above either by itself or through an auditor appointed by the Authority and the cost of audits shall be borne by the concerned entity. |

Certified audit reports are to be submitted to the Authority upon request or at time-periods specified by the Authority. In addition to the above audits, the Regulation empowers the Authority to conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

Thus, the Regulation mandates all the entities, involved in the authentication ecosystem, to keep their information systems in complete compliance with UIDAI standards and UIDAI in its turn should monitor the conformity through independent audits.

Further, Aadhaar (Data Security) Regulations stipulates that UIDAI should specify the security measures to be adopted by the Registrars, EAs, REs, and ASAs and should monitor compliance of security requirements through internal audits or through independent agencies. UIDAI empaneled (April 2018) M/s Deloitte Touché Tohmatsu India LLP (DTTILLP) as the agency to perform Information Security Assessment of all UIDAI Authentication Ecosystem Partners for a period of three years. As per the arrangement, the Authentication Ecosystem Partners would reach out to DTTILLP individually to initiate Information Security Assessment stipulated in the Aadhaar Authentication Regulations 2016. The agency will perform the Information Security Assessment once in a year and submit its Audit Report to the entity concerned. DTTILLP was to communicate to UIDAI at the end of every month the names of the audited partner.

Details of the audit of the REs and ASAs conducted during the five years of audit coverage are in **Table 5.2**.

**Table 5.2: Details of IS audit of REs and ASAs**

| Year | Requesting Entities | | | Authentication Service Agencies | | |
|---|---|---|---|---|---|---|
| | Agencies | Agencies whose audit was done by IS auditor | Agencies whose audit was done by UIDAI | Agencies | Agencies whose audit was done by IS auditor | Agencies whose audit was done by UIDAI |
| **2014-15** | 92 | NA[46] | NA | 16 | NA | NA |
| **2015-16** | 223 | 2 | NA | 23 | NA | NA |
| **2016-17** | 355 | 121 | 8 | 27 | 3 | 1 |
| **2017-18** | 308 | 110 | 29 | 26 | 3 | 3 |
| **2018-19** | 204 | 106 | 8 | 27 | 9 | 1 |

Analysis of the above data showed that no REs or ASAs had their operations audited annually either by themselves through a certified Information Systems auditor or by UIDAI.

Thus, it was evident that while UIDAI regulations stipulated annual audit of the operations and systems of both REs and ASAs by Information Systems auditor, compliance was very poor. UIDAI also failed to invoke its prerogative to audit the operations, infrastructure, systems and procedures of the REs and ASAs, either by itself or through audit agencies appointed by it. As such it was unable to derive required assurance that the entities involved in the authentication ecosystem, are maintaining their information systems in complete compliance with UIDAI standards.

UIDAI informed (January 2020) that the MoUs between UIDAI and Registrars contain provisions for periodic audit of enrolment processes. It stated that the ROs carry out audit and inspection of enrolment operation of Registrars, EAs and audit of the Self-Service Update Portal (SSUP) and back end services rendered by BPO. The reply was not relevant to the observation as it deals with MoUs between UIDAI and Registrars and relates to the adherence to enrolment processes whereas, the audit observation relate to requirement for IS audits under the Authentication Regulations, of authentication related operations of the REs and ASAs.

UIDAI further intimated (October 2020) that there had been a steady increase in submission of IS Audit Reports by AUAs i.e., from about 35 *per cent* in 2016-17 and 2017-18 to 52 *per cent* in 2018-19 and that it was pursuing this aspect with the REs and sensitizing them about the significance of the audits through training sessions.

UIDAI accepted the recommendation for conducting audit of existing REs and ASAs by the auditor appointed by it within a cycle of three years subject to the present constraints posed by Covid-19 pandemic. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

**Recommendation:** ***UIDAI may ensure that each of the existing REs & ASAs are audited by UIDAI or by the Auditor appointed by it within a cycle of three years so as to provide adequate assurance about compliance to its Regulations.***

[46] NA means- Data not available at UIDAI.

### 5.2.2 Information System Audit of Client Applications' Systems storing biometric data not ensured

***UIDAI could not provide adequate assurance that REs & ASAs accessing and storing the personal information of Aadhaar holders through the Non-Registered Biometric Devices, used prior to April 2018, had been addressed by them despite issue of directions (June 2017) mandating IS audits of client systems.***

UIDAI directed (January 2017) all AUAs/ASAs that with effect from 1 June 2017, authentication requests would be accepted only through "Registered Devices[47]" certified by STQC (Standardization Testing and Quality Certification). An important feature of the Registered Device was that it could encapsulate activities like biometric capture, signing and encryption of biometrics etc. within it. Hence, use of Non-Registered Devices will be putting resident's privacy at risk. UIDAI further instructed (February 2017) that all AUAs/ KUAs should ensure that the client applications used by sub-AUAs or other entities providing authentication services, are not capable of storing biometric data of the Aadhaar holder and the biometrics/PID block is encrypted at the frontend device/client level. The AUAs/ KUAs were to ensure that the client application does not replay any authentication request with stored biometric data under any circumstance and an information systems auditor(s), certified by STQC/ CERT-IN[48] should audit the client application. The compliance audit report was to be submitted to UIDAI and the sub-AUAs would access authentication services only through duly audited client applications. The AUAs/ KUAs were to ensure compliance to the directions and submit audit report along with a certificate duly signed by their Chief Executive Officer to UIDAI by 31 March 2017. Ensuring adherence to these directions was critical because use of Non-Registered Devices would be putting resident's privacy at risk. The timeline to complete the upgrade of applications to Registered Device for AUAs/ KUAs was initially up to May 2017 and further extensions were granted till April 2018 when all the Non-Registered Devices were deactivated.

Audit was informed (July 2020) that UIDAI had not received any audit reports from any AUAs/ ASAs within the stipulated date, in compliance of their instructions of February 2017 Further, to our query on how UIDAI ensured that the front-end devices used for e-KYC were not capable of storing biometric/PID, Audit was informed that Aadhaar (Authentication) Regulation stipulates that the client application should package and encrypt the input parameters (Aadhaar number or any other identifiers provided by the requesting agency), into PID block before transmission. Therefore, it was mandatory for the requesting agencies to ensure compliance to the provisions of the Aadhaar Act and associated regulations and instructions issued by UIDAI.

---

[47] Public devices are biometric capture devices that provide Aadhaar compliant biometric data to the application, which, in turn encrypts the data before using for authentication purposes. A registered Device is a public device with additional features compared to public device like Device identification, eliminating use of stored biometrics and having a standardized RD service. Registered devices MUST ensure that; i.) there should be no mechanism for any external program to provide stored biometrics and get it signed and encrypted and ii.) There should be no mechanism for external program/probe to obtain device private key used for signing the biometrics.

[48] Indian Computer Emergency Response Team is a functional organization of the Ministry of Electronics and Information Technology. Apart from the objective of securing the Indian cyber space CERT-In provides Security Quality Management service also.

UIDAI further stated (October 2020) that implementing a significant technical change across the country without disrupting ongoing services required a calibrated approach and could take longer time than envisaged initially. UIDAI completed implementation of biometric registered devices for the authentication system by April 2018 thereby ensuring that the biometrics were encrypted at the device itself before sending it to client application. No RE could perform authentication using non-registered device. Thus, there was no risk of the client application storing biometric data, thereafter. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Audit noted that during the period April 2017 to March 2018, nearly 385 Crore e-KYC transactions were undertaken by UIDAI. This was more than 76 *per cent* of the cumulative e-KYC transactions done since the year 2013-14. There is no assurance that many of these transactions were done using client applications that were capable of storing biometric data of residents.

Though UIDAI had claimed that it had completed implementation of biometric registered devices for the authentication system by April 2018, there was no system to confirm that the client applications used by authentication ecosystem partners for providing authentication services prior to April 2018, were not capable of storing biometric data of the Aadhaar number holders. As such, there was inadequate assurance that the risk of ASA/ AUAs/ sub-AUAs accessing and storing the personal information of Aadhaar holders through the earlier Non-Registered Devices, was addressed by UIDAI despite issuing directions in June 2017 mandating IS audits of client systems.

**Recommendation:** ***UIDAI may consider suspension of the services of REs and ASAs if they fail to conduct annual audit in time as prescribed by the Regulations 2016.***

### 5.2.3 Security and safety of data in Aadhaar vaults

***Aadhaar numbers and any connected Aadhaar data were to be stored mandatorily on a separate Aadhaar Data Vault. UIDAI could not provide reasonable assurance that the entities involved adhered to the procedures.***

Security of CIDR information requires highest importance for safeguarding resident data. The confidentiality, integrity and availability of the information should be in controlled manner. UIDAI has obtained ISO 27001:2013 certification from STQC by establishment of Information Security Management System. UIDAI-CIDR has also been declared as "Protected System" by National Critical Information Infrastructure Protection Centre (NCIIPC) adding another layer of IT security assurance. However, safeguarding the Aadhaar data with the same level of security measures has to be maintained throughout the Aadhaar Ecosystem, including the authentication partners.

With a view to enhance the security level for storing the Aadhaar numbers, UIDAI mandated (July 2017) all AUAs/KUAs/Sub-AUAs and other entities who are collecting and storing the Aadhaar numbers for specific purposes, to implement Aadhaar vaults[49]. UIDAI also prescribed

[49] Aadhaar Data Vault is a centralized storage for all the Aadhaar numbers collected by the AUAs/ KUAs/ Sub-AUAs/ or any other agency for specific purposes under Aadhaar Act and Regulations, 2016. It is a secure system inside the respective agency's infrastructure accessible only on need-to-know basis.

the procedure for implementation of Aadhaar vaults and non-compliance would attract general penalty provisions of the Aadhaar Act. In addition, UIDAI could also levy financial disincentives as per the conditions provided in the AUA/ KUA agreement. Since the entities were permitted to store Aadhaar numbers along with the demographic information and photo of the Aadhaar holder, UIDAI had stipulated security and safety measures, which the entities were required to comply with while implementing Aadhaar vaults.

For verification of compliance to the above mentioned requirements and systems put in place to monitor compliance with directions by user agencies/ entities on implementing Aadhaar Data Vaults, UIDAI informed Audit (July 2020) that REs were to ensure that the objective of secure storage of Aadhaar numbers is met. UIDAI has not specified any encryption algorithm or key strength for the encryption of Aadhaar Data Vault. It further mentioned (October 2020) that Aadhaar Data Vault (ADV) was not a specific product but a process and a concept for storage of Aadhaar numbers in a secure manner and its implementation was monitored through Audit Reports submitted by the REs. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

The above position indicated that UIDAI had not established any measures /systems to confirm that the entities involved adhered to procedures and was largely dependent on Audit Reports submitted to them. They had not independently conducted any verification of compliance to the process to derive a satisfactory assurance.

Aadhaar number is a lifetime identity for Indians and is used to avail various services involving financial transactions, as such unauthorized access to Aadhaar number can be misused in many ways. Hence UIDAI may ensure the implementation of Aadhaar Data Vault by instituting periodic audit to enhance the security for the data stored by user organizations. It should deal with non-compliance strictly as per the Act and as per conditions in the agreement with AUAs/ KUAs

**Recommendation:** ***UIDAI may ensure the implementation of Aadhaar Data Vault process and institute/carry out periodic audits independently, to enhance the security of Aadhaar number storage data by user organizations. UIDAI may deal the cases of non-compliance of directions as per the Act and as per conditions in the agreement with AUAs/ KUAs (Authentication User Agencies and e-KYC User Agencies)***