Chapter 2 Scope of Audit, Audit Objectives and Methodology

2.1 Scope of Audit

The Performance Audit included assessment of the Enrolment & Update Ecosystems as well as the Authentication Ecosystems of the UIDAI for the period from 2014-15 to 2018-19. The figures have been updated wherever received upto March 2021. Audit scrutinised the processes beginning right from the enrolment, upto delivery of Aadhaar number and subsequent use of the authentication services. The systems put in place for maintaining security and confidentiality of data were also subject to audit examination. In addition, audit also examined selectively, the procurement of infrastructure for the project.

2.2 Audit Objectives

The main audit objectives of the Performance Audit were to ascertain whether:

1. UIDAI has developed comprehensive regulations to comply with the responsibilities entrusted under the Aadhaar Act.
2. Ecosystem put in place for issue of Aadhaar and Authentication services functioned efficiently and in compliance with the statutory requirements.
3. UIDAI has put in a system to monitor the performance of the IT systems associated with its operations.
4. Contract management system in UIDAI for procurement of IT and other services is in conformity with government regulations and is executed to achieve economy and efficiency in operations.
5. Complaint redressal mechanism set up by UIDAI for handling Aadhaar related grievances was effective.

2.3 Audit Criteria

Important criteria adopted for the Performance Audit were:

a. Cabinet Approval on the formation of UIDAI and decisions of Expenditure Finance Committee (EFC).

b. Provisions of Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and subsequent Amendments.

c. Relevant provisions under General Financial Rules (GFR), 2005 and its revised version GFR 2017, which have elaborately stipulated procedures for procurement, maintenance of stock and stores, their disposals, etc.

d. The Procurement Manual 2014 (effective from 01 April 2014) issued by UIDAI, contains the principles and procedure relating to procurement of goods and services for purposes of UIDAI and is drawn from the Rule 135 of the GFR 2005.

e. The Aadhaar (Enrolment and Update) Regulations, 2016.

f. The Aadhaar (Authentication) Regulations, 2016.

g. The Aadhaar (Data Security) Regulations, 2016.

h. Aadhaar (Sharing of Information) Regulations, 2016

i. Subsequent Amendments to the above regulations and any other instructions/notifications/Regulations issued by Government/UIDAI, which have a bearing on the project and functioning of UIDAI.

2.4 Audit Methodology

The Performance Audit commenced with an entry conference with the top management of UIDAI at UIDAI Headquarters at New Delhi in February 2019 where the scope of the audit, audit objectives etc. were explained to the Management. Files and records, maintained at UIDAI HQ, its ROs[9] and at UIDAI Tech Centre at Bengaluru were reviewed in audit.

We selected contracts for scrutiny based on statistical sampling techniques. Besides, examination of documents, we obtained information by way of replies to audit questions furnished by the auditee and through meetings with key personnel of UIDAI involved in its various operations.

On completion of Audit, we discussed important observations with the UIDAI management in an Exit Meeting in October 2020. Auditee's response given during the Exit Meeting and by way of a written reply has been suitably included in this Report. The statistical information has been updated to 31 March 2021.

The reply of the Ministry of Electronics and Information Technology (MeitY) furnished in June 2021 has also been taken into consideration in finalizing the report.

2.5 Good Practices

UIDAI has provided an identity document to over 125 crore residents of India within a decade of issue of the first Aadhaar (September 2010) in coordination with a large number of agencies/ entities spread across the country. UIDAI has established the Information Security Management System and obtained the ISO 27001:2013 by STQC and the National Critical Information Infrastructure Protection Centre (NCIIPC) has declared its CIDR as "Protected System" adding another layer of IT security assurance.

We noted that UIDAI has a system of imposing financial penalties on its enrolment ecosystem partners for deficient/ defective quality of work. Complaints of overcharging of residents are followed up and financial disincentives are imposed on Registrars. It was observed that payments to Registrars are released only after crosschecking with the list of successful generation of Aadhaars obtained from UIDAI Tech Center.

Features like the Virtual ID and Biometric Locking facility provides more leeway to Aadhaar holders while availing Aadhaar related services. The Virtual ID is a temporary and revocable 16-digit random number and is mapped with the Aadhaar so that it can be used in place of Aadhaar for authentication The Biometric Locking facility helps an Aadhaar holder to lock/unlock his/ her biometrics whenever he/ she wishes. These initiatives help in enhancing confidence of Aadhaar holders while using the ID.

[9] Except Guwahati RO

In 2019, "Aadhaar Seva Kendras" (ASK) were introduced in 41 select locations in the country to act as a single stop destination for all Aadhaar services for the residents. These ASKs were in addition to 35,000 already available Aadhaar enrolment and Update Centers.

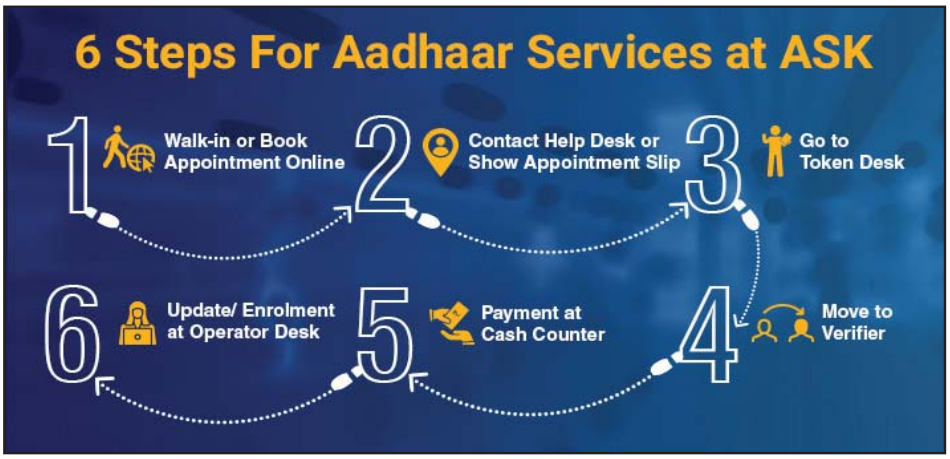

Image courtesy: UIDAI

The ASKs offer dedicated Aadhaar enrolment and update services to residents on all seven days of the week.

2.6 Acknowledgement and Constraints

We acknowledge the support and cooperation extended by the Management of UIDAI to the audit team during the course of audit. A detailed presentation on the functioning of the Authority was given for understating of the Audit Team. The records/ data requisitioned by Audit Team were generally furnished but audit witnessed several instances of inordinate delay/ non-supply of records which impeded in the audit exercise. Records, which could not be accessed included files related to Information Technology-Information System Security, Aadhaar Document Management System, destruction of documents collected at the time of enrolment, details of authentications and its accounting, fixation of rates/ charges for authentication and enrolment & update activities, grievances /complaints of customers, audit reports of stake holders (e.g. enrolment centres or ASAs/AUAs) etc. We also appreciate the support provided in updating the statistical and other information till March 2021.

UIDAI expressed difficulties in providing data for period prior to formation of UIDAI (July 2016) as an Authority under Aadhaar Act. Intermittent supply of data, delayed submission and partial responses to audit queries had hindered the smooth completion of audit process. We could not provide reasonable assurances on the selection process of vendors appointed by UIDAI for managing the vital services in the roles of Managed Service Providers, Data Centre Development agencies and Aadhaar Documents Management System partners or Government Risk Compliance and Performance – Service Providers. However, we relied on the UIDAI write ups and the scrutiny of files to arrive at a conclusion that the service partners for providing the services[10] were selected in competitive manner by following the prescribed rules, procedures and due diligence. The contracts for supply of professional resources entered into with NISG were on nomination basis.

[10] The services which were selected for audit scrutiny following the decided samples

Therefore, in keeping with the scope of the CAG's Regulations on Audit and Accounts, to the extent data and information/files were not produced to the audit, we could not derive our assurance on the areas mentioned above.