F. no.: HQ-13031/1/2022-AUTH-I HQ (Comp No. 13927)/3028

Unique Identification Authority of India

(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Gole Market, New Delhi – 110001
Dated: 04.11.2025

Circular No. 14 of 2025

Subject: Revised guidelines for hosting Hardware Security Module (HSM), Aadhaar Data Vault (ADV) and authentication application on premises and cloud infrastructure for Aadhaar Authentication Ecosystem.

This circular superseded the UIDAI circular no. 11020/205/2017-UIDAI (Auth-I) dated 25.07.2017, Circular 8 of 2025 dated 18.07.2025 on ADV implementation and shall be read in continuation of UIDAI circular No. 11020/204/2017-UIDAI (Auth-I) dated 22.06.2017 on HSM implementation.

2. All requesting entities (REs) are directed to mandatorily store Aadhaar numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and demographic data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where Aadhaar Number and any connected data will be stored.

3. Entities are allowed to securely store UID Tokens or any relevant demographic data and/or photo of the Aadhaar Number Holder in their local database in encrypted manner with Cryptographic Algorithms (Symmetric/Asymmetric Encryption) as long as Aadhaar Number is not stored in those systems.

4. Requesting entities are strictly prohibited for storing Aadhaar number or related data from the requested inputs by the Aadhaar number holder in Authentication/eKYC request.

5. The ADV implemented by a requesting entity must be hosted on either of the following

(a) on-premises (within the secure premises of the requesting entity/technical service provider);
(b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India, list of those Cloud Service Providers (CSP) are available at *https://www.ambud.meity.gov.in* ; and
(c) ADV as-a-service provided by UIDAI Requesting Entities.

6. In case of GCC platform-based cloud implementation or ADV as-a-service based implementation, the annual System and Organization Controls (SOC 2) Type II audit of the cloud infrastructure must be conducted by Cert-IN empanelled auditor agency authorized for cloud security audit and this has to be ensured by the concerned requesting entity.

7. Requesting entities must ensure the following for ADV implementation:

(a) The GCC provider or the entity providing ADV as-a-service must be compliant with UIDAI security and privacy standards and ensure complete logical segregation of ADV for each requesting entity.

(b) Each Aadhaar number is to be referred by an additional key called as Reference Key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.

(c) All business use-cases of entities shall use this Reference Key instead of Aadhaar number in all systems where such reference key need to be stored/mapped, i.e. all tables/systems requiring storage of Aadhaar numbers for their business transactions should from now onwards maintain only the reference key. Actual Aadhaar number should not be stored in any business databases other than ADV.

(d) The data in ADV shall be stored in a single logical instance for each entity with the corresponding reference key which must be generated and used. Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

(e) Aadhaar data must be stored in an encrypted format using strong algorithms like AES-256 (*or* higher) *or* as specified in latest Authentication API.

(f) High Availability and Disaster Recovery (HA/DR) shall be in place for the ADV with the same level of security along with dual redundant connectivity to the ASAs. It should have sufficient bandwidth based on respective anticipated transaction volume.

(g) The Aadhaar Data Vault containing Aadhaar number/data and the referencing system must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.

(h) Only trusted communication channels and secure APIs/microservices, shall be used for data access in vault. All access must be routed through authenticated applications with appropriate user authentication, authorization and logging mechanisms.

(i) Robust access control, monitoring and alerting systems must be implemented to detect and prevent unauthorized access to ADV. Ensure strict implementation of Identity and Access Management (IAM) so that only authorized personnel and systems can access the vault. All access must be logged and monitored.

(j) The Aadhaar Data Vault should support mechanisms for secure deletion/update of Aadhaar number and corresponding data if any as required by the data retention policy of the entities.

(k) The chosen Reference Key generation method is to ensure that the recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or number of reference keys. Hashing of Aadhaar numbers is not allowed to be used as Reference keys.

8. Requesting entities and Authentication Service Agencies (ASA) must mandatorily implement the Hardware Security Module (HSM) for cryptographic operations (such as signing of authentication request, encryption/decryption of ADV data, decryption of eKYC response data or any other operation as mandated by UIDAI time to time). The HSM must be hosted as either of the following:

   (a) on-premises (within the secure premises of the requesting entity),
   (b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India,
   (c) as HSM services provided along with ADV as-a-service by any entity.

9. Requesting entities and ASAs must ensure the following for HSM implementation:

   (a) It must be FIPS 140-2 Level 3 certified or higher,
   (b) It must be logically isolated for each requesting entity/ASA independently,
   (c) It must support:
      (i) Key Generation
      (ii) Secure Key Storage
      (iii) Multifactor, Multirole Access Control and Audit Logging

10. Aadhaar authentication applications or any module handling authentication data shall only be hosted on-premises (within the secure premises of the requesting entity) *or* on a GCC platform-based cloud, empaneled by MeitY, Govt. of India.

11. Requesting Entities and ASAs are advised to refer the latest list of MeitY-empaneled GCC services provider, available at: *https://www.ambud.meity.gov.in*. This list is maintained and updated by MeitY.

12. Additional information and clarifications can be found in the Frequently Asked Questions (FAQ) section accessible through below mentioned link – https://uidai.gov.in//images/FAQs_Aadhaar_Data_Vault_03112025_v10.pdf

13. This issues with the approval of competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

To:

1. All requesting entities and Authentication Service Agencies in Aadhaar Authentication Ecosystem

Copy, for information, to:

1. Secretaries in charge of Ministries and Departments in Government of India (as per list attached)
2. Chief Secretaries of State Governments (as per list attached)
3. Chief Secretary, Government of Jammu and Kashmir / National Capital Territory of Delhi / Puducherry / Andaman and Nicobar Islands Administration
4. Advisor to Administrator, Chandigarh Administration
5. Advisor to Lieutenant Governor, Ladakh Administration
6. Administrator, Dadra and Nagar Haveli and Daman and Diu Administration / Lakshadweep Administration
7. Technology Centre, UIDAI, Bangalore
8. Regional Offices, UIDAI