F. no.: HQ-13031/1/2022-AUTH-I HQ (Comp No. 13927)
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Gole Market, New Delhi – 110001
Dated: 18 .07.2025

Circular No. 8 of 2025

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

This circular shall be read in continuation of UIDAI circular no. 11020/205/2017-UIDAI (Auth-I) dated 25.07.2017 on ADV implementation and circular no. 11020/204/2017-UIDAI (Auth-I) dated 22.06.2017 on HSM implementation.

2. All requesting entities (REs) storing Aadhaar numbers, UID Tokens and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and demographic data) are directed to mandatorily implement the ADV.

3. Storage of Aadhaar number, UID Token or any Aadhaar demographic data received after successful Authentication or eKYC shall only be permitted within the ADV. 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.

4. 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);
(b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India; and
(c) ADV as-a-service provided by an entity.

5. In case of GCC platform-based cloud implementation or ADV as-a-service based implementation, annual System and Organization Controls (SOC 2) Type II audit of the cloud infrastructure must be ensured by the concerned requesting entity.

6. 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) 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.
(c) Aadhaar data must be stored in an encrypted format using strong algorithms like AES-256 or above.
(d) 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.
(e) Only trusted communication channels, and secure APIs/microservices, shall be used for data access in vault.

(f) All access must be routed through authenticated applications with appropriate user authentication, authorization and logging mechanisms.

(g) 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.

7. 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, empanelled by MeitY (Ministry of Electronics and IT), Govt. of India,

(c) as HSM services provided along with ADV as-a-service by any entity.

8. 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

9. The application should rotate the key, and the requesting entity/ASA must have a mechanism in place for the prevention of unauthorized substitution of keys.

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 MeitY-empanelled platform.

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

12. 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 to:

1. Technology Centre, UIDAI, Bangalore
2. Regional Offices, UIDAI