Frequently Asked Questions (FAQs)
Aadhaar Data vault (ADV) / Hardware Security Module (HSM)
(Updated as on 03.11.2025)

1. What do you mean by Aadhaar related data?

Aadhaar related data means Aadhaar number along with demographics details i.e. Name, DoB, Gender, Address and Photo, email ID or mobile number.

2. What are reference keys?

In order to minimize the footprints of the Aadhaar numbers and its connected data within the infrastructure of REs, each Aadhaar number is to be referred by an additional key called Reference Key. These keys will replace Aadhaar numbers in the organizations ecosystem. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.

3. What is Hardware Security Module (HSM)?

A Hardware Security Module (HSM) is a tamper-resistant physical device mandated for securely generating, protecting, and managing cryptographic keys used in Aadhaar authentication and e-KYC transactions. All private keys for digital signing of authentication XML and for decrypting e-KYC data must reside only within the HSM, never outside it, to ensure high-grade security and compliance with FIPS 140-2 Level 3.

4. What is objective of HSM?

The objective of a Hardware Security Module (HSM) is to provide a dedicated, tamper-resistant environment for the secure generation, storage, and management of cryptographic keys.

5. Can a single HSM be shared between AUA/KUA and their Sub-AUAs/Sub KUAs?

Sub-AUA/Sub-KUA may use their respective AUA's/KUA's HSM, subject to adherence to the following stipulations:

(a) The HSM configuration must ensure logical isolation for each RE.

(b) Dedicated cryptographic keys for each RE shall be provisioned and maintained within the logical isolation of HSM.

(c) Implementation of Identity & Access Management (IAM) to control and monitor all access to cryptographic keys and associated interfaces.

(d) Multifactor authentication, Multirole-based Access Control and robust Audit Logging must be enforced to safeguard access and to provide traceability for all cryptographic operations.

6. Can existing HSMs be used for storing the encryption keys?

REs may use their existing HSM for storing the keys used for encryption of data stored in Aadhaar data vault. However, these keys cannot be shared with any other RE, except for their authorized Sub-AUAs/KUAs. To facilitate this, the AUAs/KUAs must provide a separate logical partition within the HSM for each of its Sub-AUAs/Sub-KUAs to store the respective encryption keys including IP whitelisting. REs is responsible for ensuring the security of the partitions that store Aadhaar data vault keys.

7. Is it allowed to store Aadhaar Number and connected data in other systems than vault if the system provides HSM level encryption for storage / usage of Aadhaar Number

All REs are directed to mandatorily store Aadhaar numbers along with any connected Aadhaar data (i.e. eKYC XML containing Aadhaar number and its demographic data) in ADV implemented with HSM. If the RE wants to convert the existing Database into Aadhaar Data Vault (ADV) complying to latest Circular issued by UIDAI time to time, such RE may do so. In that case, the RE must ensure that the Aadhaar numbers are only stored on this ADV and removed from other databases.

8. What is Aadhaar Data Vault?

Aadhaar Data Vault is a separate secure database/vault/system for Aadhaar data (i.e. eKYC XML containing Aadhaar number and its demographic data) received by the requesting entities (RE) for specific purposes approved under Aadhaar Act, 2016 and associated Regulations thereunder. It is established along with HSM.

9. What is the objective of Aadhaar Data Vault?

Objective of Aadhaar Data Vault is to minimize footprints of the Aadhaar numbers by encrypting it and its connected data and before securely storing it within the infrastructure of REs.

10. Who needs to implement Aadhaar Data Vault?

All REs storing full Aadhaar number along with any connected Aadhaar data in accordance with the Aadhaar Act, 2016 and associated regulations and any directions/guidelines issued hereafter are required to implement Aadhaar data vault.

11. Are there any implementation guidelines for Aadhaar Data Vault?

Yes, UIDAI has issued implementation guidelines for ADV which is published under Authentication documents at uidai.gov.in on below mentioned link: (https://uidai.gov.in/en/ecosystem/authentication-devices-documents/authentication-document.html)

12. What data needs to be stored mandatorily in ADV?

Full Aadhaar number along with any connected Aadhaar data (i.e. eKYC XML containing Aadhaar number and its demographic data) received by the requesting entities (RE) from e-KYC response must be stored only within ADV. Aadhaar number or related data provided by Aadhaar Number Holder (ANH) in Authentication application submitted for authentication (mobile/web) is prohibited to be stored by the RE in any form.

13. For Sub-AUAs/Sub-KUAs, is it mandatory to implement a dedicated ADV at their end or can they utilize their AUA's/KUA's ADV?

Sub-AUAs/Sub-KUAs may implement their own ADV or use their respective AUA's/KUA's ADV as-a-service subject to implementation of Identity & Access Management (IAM) and ensuring logical segregation. In addition, Sub-AUAs/Sub-KUAs are fully responsible for ensuring compliance with respect to the Aadhaar Act, 2016 and associated regulations as amended thereafter.

14. Can an AUA/KUA access the data in ADV for their Sub-AUAs/Sub-KUAs?

No, AUA/KUA cannot access any data in ADV of their Sub-AUAs/Sub-KUAs.

15. Is it required to replace all the Aadhaar number with the reference keys which are being used in the existing infrastructure in multiple databases?

RE needs to create an Aadhaar data vault and replace Aadhaar numbers in all existing databases with the respective reference keys even if Aadhaar number is stored encrypted in several databases within the RE.

16. Can demographic details (received from e-KYC) be stored locally if Aadhaar and UID Token are not stored with it?

Yes, demographic details can also be stored locally if Aadhaar and UID token are not stored/mapped with it by taking reasonable security safeguards to prevent breach of such data, which shall include, at the minimum, appropriate data security measures, including securing such data through encryption, obfuscation or masking.

17. Can UID Token alone (without demographic details) be stored locally?

Yes, UID token can be stored safely without encryption after its mapping with reference key by taking reasonable security safeguards to prevent breach of such data, which shall include, at the minimum, appropriate data security measures.

18. If an entity wants to store the Aadhaar pdf (received from eKYC response) locally, is it permissible from UIDAI side?

No, Aadhaar pdf (received from eKYC response) shall only be stored in encrypted manner inside ADV.

19. Who all can provide Aadhaar Data Vault as-a-service?

All existing global AUAs/KUAs (implemented a fully compliant ADV), CSPs providing ADV as a service hosted on GCC empaneled cloud or a technical service provider providing on-premises services of ADV can provide ADV as-a-service.

20. Which encryption algorithm is required for encryption of Aadhaar numbers and related data in the Aadhaar Data Vault?

The encryption algorithm and key strength required for securing Aadhaar numbers and related data in the Aadhaar Data Vault must comply with the latest UIDAI specification, API 2.5 for Authentication and eKYC. These specifications are subject to change, and regulated entities must refer to the latest UIDAI documentation for updated requirements.

21. Is it possible to use existing unique values, such as Bank account numbers or PAN numbers, for an entity to be used as reference keys?

The organization may use any reference keys as long as it can be uniquely mapped to the respective Aadhaar numbers and meets the requirement of the UIDAI Circulars regarding ADV implementation, such as Aadhaar numbers should not be predictable if corresponding reference keys or set of keys are available. Organization should consider other implications of using Bank account / PAN card as reference keys which may be local to the environment.

22. Can multiple reference keys be generated and used with a single Aadhaar?

Multiple reference keys may be generated for a single Aadhaar if there is such business case which requires to refer one Aadhaar by different reference keys in the internal ecosystem of the RE. In such cases, the RE shall ensure compliance to the other requirements specified in the UIDAI Circulars/Guidelines on the ADV, as issued by UIDAI time-to-time.

23. What is the nomenclature / convention to be followed for Unique Reference Number Generation for Aadhaar?

This is left to organization to choose nomenclature/convention as long as it ensures that the recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or numbers of reference keys. Hash of Aadhaar No. should not be used as reference key.

24. As Aadhaar number is used for carrying out DBT transactions, etc., will the Aadhaar number be continued to be used while processing the transactions?

Aadhaar number may be used wherever necessary to process the transactions, however when the transaction related data or Aadhaar related data is stored, Aadhaar numbers should not be stored in any other storage than Aadhaar Data Vault.

****