Unique Identification Authority of India

Frequently Asked Questions (FAQs) – Aadhaar Data vault / Reference keys

Ref: UIDAI circular dated 25.07.2017

1. What is Aadhaar Data Vault

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.

2. What is the objective of Aadhaar Data Vault

Aadhaar number has been identified as "Identity Information" under the Aadhaar Act 2016 and can uniquely identify residents in India. Since Aadhaar number is a lifetime identity for Indians and shall be used to avail various services including services involving financial transactions, unauthorized access to Aadhaar number may be misused in many ways.

Objective of Aadhaar Data Vault is to reduce the footprint of Aadhaar numbers within the systems / environment of the organization hence reduce the risk of unauthorized access.

3. Does Aadhaar Data Vault refer to any technology?

Aadhaar Data vault is a concept for storage of Aadhaar numbers in one particular storage within the environment of the organization to reduce the footprint of Aadhaar numbers. It does not refer to any technology. The decision of procuring a technology to implement Aadhaar Data vault or implementing Aadhaar Data vault internally lies with the respective organization.

4. Who needs to implement Aadhaar Data Vault

All agencies which store Aadhaar number are required to create an Aadhaar data vault. These agencies may or may not be AUAs/KUAs/Sub-AUAs. They could be an organization that stores Aadhaar numbers for internal identification purposes such as attendance management, linking with PF etc. All the agencies that store Aadhaar numbers in a structured and electronic form such as a Database need to implement Aadhaar Data Vault.

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

The implementation of Aadhaar Data vault needs to be decided by the respective organization with the assistance of their internal technical teams. The implementation should meet the objective of the circular.

6. Which encryption algorithm is required for encryption of Aadhaar numbers and related data in the Aadhaar Data Vault as per the requirement of the circular?

UIDAI has not specified any encryption algorithm or key strength for the encryption of Aadhaar data vault, however other standards / specifications of UIDAI may be referred for algorithm and key length such as Auth api specifications or eKYC api specifications where it states RSA 2048 for Public key encryption and AES 256 for symmetric encryption (this is as per current version and the standards may change with time). Industry standards / Best practices should be followed in absence of such specifications.

7. Is it required to have separate VLAN for the Aadhaar Data Vault

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. Agencies may create only a virtual separation for Aadhaar data vault, however such agencies need to ensure they comply with the requirements of the notice such as access control, logical segregation in zones etc.

8. What are reference keys

In order to reduce the footprint of Aadhaar numbers in the ecosystem, each Aadhaar number is to be referred by an additional key called as Reference Key. These keys will replace Aadhaar numbers in the organizations ecosystem and mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.

9. Is it possible to use existing unique values for a user to be used as reference keys. Such as Bank account numbers or PAN numbers 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 circular 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.

10. Can existing HSMs be used for storing the encryption keys

Agencies may use the existing HSMs. HSMs used to store the keys for encryption of Aadhaar data vault cannot be shared with any other agency / legal entity. Security of the partitions storing Aadhaar data vault keys need to be ensured by the agency.

11. If the Aadhaar number needs to be sent to UIDAI server or NPCI , how would it be communicated using reference keys?

Reference keys are local to agency/organization and is not required to be shared with UIDAI server or NPCI. Wherever Aadhaar number needs to be sent outside the agency for a genuine business, it may be sent to complete the transaction. However when the details of the transaction are to be saved within the environment, corresponding reference keys should be stored instead of Aadhaar numbers. After completion of the transaction, reference key for the corresponding Aadhaar number needs to be obtained from the Aadhaar Data vault through APIs.

12. How are the scanned/physical copies of the Aadhaar numbers be stored in the Aadhaar Data vault?

For the agencies which store the scanned images of Aadhaar cards or physical copies of Aadhaar cards as per TRAI / RBI etc., the storage of scanned images or physical cards do not come in scope of this notice or requirement. The agencies need to keep the scanned copies encrypted and ensure security of both scanned copies and physical copies as per Aadhaar Act 2016 and Regulations. Agency should ensure compliance to the security and privacy requirements for storage of scanned images or hard copies as per Aadhaar Act 2016 and Regulations.

13. Is it allowed to store Aadhaar number as masked value in any systems apart from Aadhaar Vault? Ex : 1234 ** 5678**

Aadhaar numbers either in encrypted form or masked form should not be stored in any other storage except Aadhaar Data vault.

14. Can Aadhaar number be used for resetting password as security questions?

Some agencies are storing Aadhaar number to be able to answer the security question for a password reset request. These agencies cannot store the Aadhaar number anywhere else apart from the Aadhaar data vault and they come in scope of the requirement. However if these agencies want to store only the last 4 digits of the Aadhaar number for internal authentication purposes such as a security question they may store the same. In no situation Aadhaar number except the last 4 digits may be stored outside the Aadhaar Data vault.

15. Can multiple reference be generated and used with a single Aadhaar card

Multiple reference keys may be generated for a single Aadhaar if there is such business case which requires to refer one Aadhaar number by different reference keys in the internal ecosystem of the agency. In such case, the agency shall ensure compliance to the other requirements of the circular.

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

Agency 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 agency.

17. Aadhaar (Authentication) regulations 2016 require to store the Aadhaar number in the transaction logs. Is it required to replace all these Aadhaar number with the reference keys?

For the requirement of mandatory storage of Aadhaar number in the logs for authentication / e-KYC transactions, the agencies need to replace the Aadhaar numbers in the Logs Databases with the corresponding reference keys. For future transactions, only reference keys shall be stored in the logs and if for any regulatory or genuine business purpose the transaction logs need to be provided outside the agency / organization same shall be provided along with the Aadhaar number.

18. There are backups already taken of the databases containing Aadhaar numbers by some agencies. Is it required to replace all the Aadhaar number with the reference keys in the back up of logs/databases already taken in the past

These agencies may continue to store such backups which have existing Aadhaar numbers as long as the data is kept encrypted.

19. Can the hash of Aadhaar card be used as reference keys

Agency / Organization may choose any method for generation of reference key. 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. It is suggested that a UUID (Universally Unique Identifier represented via hex string) scheme be used to create such reference key so that from such reference key, Aadhaar number can neither can be guessed nor reverse engineered.

20. Which industry standard to be followed for key generation/ encryption

The organization may choose appropriate industry standard as per its requirement as long as it meets the requirement of the circular.

21. Whether a particular agency can provide reference key provisioning as a central service to its Sub – AUAs?

Since the AUAs are already obligated for the compliance of its Sub-AUAs and already has all Aadhaar numbers of its Sub-AUAs as part of the transaction logs, AUAs may provide reference provisioning as a central service to its Sub-AUAs. Access to mapping databases / Aadhaar Data vault need to be on a need to know basis. Other risks of providing reference key service as a central service need to be considered by the Sub-AUA / AUA.

22. Can HSM service be stored on cloud and provide service to sub-AUA's

Since an AUA already is obligated for the compliance of its Sub-AUAs and already has all Aadhaar numbers of its Sub-AUAs as part of the transaction logs, HSM may be provided by the AUA as a central service to its Sub-AUAs. In no other circumstance HSM shall be shared with other agencies / organizations as it implies sharing of Aadhaar numbers and other related data with that organization.

23. Can we use the same VM for business application & Aadhaar vault application

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. Compliance with circular and Aadhaar act needs to be ensured.

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

All entities / agencies are directed to mandatorily store Aadhaar Numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and data) only on a separate secure database/vault/system. Aadhaar numbers shall not be stored in any other systems. If the agency wants to term the existing Database as Aadhaar Data vault and can meet the other requirements of the circular, such agency may do so. In that case the agency must ensure that Aadhaar numbers are only stored on this database and removed from other databases.

25. Can we use any method to generate reference key or only UUID to be used as recommended in the circular?

Any method may be used to generate the reference key as long as it meets the requirements of the circular.

26. What is the nomenclature / convention to be followed for Unique_Ref_Number_Generation for Aadhaar?

This is left to organization to choose nomenclature/convention as long as it ensure that the recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or number of reference keys.

27. By when agencies must be compliant to the system of implementing Aadhaar Vault?

The organizations must start the implementation of the Aadhaar Data vault immediately. The same shall be checked during the next independent audit to be conducted by the agency itself or by UIDAI.

28. Which version to opt for in the technical specification of HSM. Ex: FIPS 140-2 Level 2 or FIPS 140-2 Level 3 HSM?

UIDAI has not recommended any specifications for HSM. Organization may follow the Industry best practice such as NIST etc.

29. As Aadhaar number is used for carrying out DBT transactions, AEPS transactions etc., will the Aadhaar number will 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.

30. At the time of transaction processing the application will refer to Aadhaar vault only to derive the account to which the amount is to be credited or debited and the transaction will be carried out accordingly.

The Aadhaar Data vault should ideally maintain only the mapping of Aadhaar numbers and corresponding reference numbers. Hence any access to data vault (except for maintenance purposes / Administration purposes) should only be to refer this mapping.

31. Will there be an audit required after the implementation of Aadhaar Data Vault.

UIDAI does not mandate an audit after the implementation of Aadhaar Data vault. However same should be checked in the next periodic external audit as per UIDAI requirement. However the agency should maintain some documentation to demonstrate that the implementation meets the requirement of UIDAI circular. This could be in the form of an internal audit from an independent team or confirmation on the points of the circular by the internal technology or security team (independent).