cpl.thalesgroup.com

THALES
Building a future we can all trust

# How to Effectively Adhere to UIDAI's Aadhaar Data Vault Compliance Mandates

## About UIDAI

The Unique Identification Authority of India (UIDAI), a Government of India statutory authority, issues Unique Identification numbers (UIDs) named "Aadhaar" to all residents of India. The 12 digit unique-identity number is based on a person's biometric and demographic data.

With the aggregation of Aadhaar data becoming a necessity for all types of Know-Your-Customer (KYC) processes in India, there has been an implosion of personally identifiable information (PII) that is used by private and public organisations to collect, process, store, and manage this sensitive data.

To ensure that the Aadhaar data is not misused by any entity, Unique Identification Authority of India (UIDAI) – the apex regulator for Aadhaar, has issued stringent data protection mandates for data fiduciaries (entities that collect the Aadhaar data) and data processors (entities that process, store, and manage the Aadhaar data).

## Decoding UIDAI's Aadhaar Data Protection Mandates

To ensure that the Aadhaar data is cohesively protected at each stage of its journey, UIDAI through its circular dated 25th July 2017 has laid down the below key mandates for data fiduciaries and processors:

1. **Aadhaar Data Vault**
   Aadhaar Numbers, and any connected Aadhaar data (like the e-KYC containing the Aadhaar Number and data), should be stored only in a separate virtual repository called the 'Aadhaar Data Vault'.
2. **Tokenization**
   Each Aadhaar Number should be represented mandatorily by a "Reference Key" using the tokenization methodology. The mapping of the reference keys with their corresponding Aadhaar Numbers should be maintained separately in the Aadhaar Data Vault only.
3. **Encryption and HSMs**
   All the information stored within the Aadhaar Data Vault should be mandatorily encrypted and the encryption keys should be stored separately in a dedicated Hardware Security Module (HSM) device only.
4. **Access Controls**
   The Aadhaar Data Vault must implement strong access controls, authentication measures, logging reports, and flagging mechanisms for instantly alerting instances of suspicious and/or unauthorised access attempts.
   Furthermore, the Aadhar Data Vault must be kept in highly restricted and isolated zones, without any connection to untrusted external networks or any other internal networks.
5. **Key Management**
   To ensure that the encryption keys do not fall in the wrong hands or get compromised in any way, centralised key management should be implemented to cohesively protect the keys throughout their lifecycle.

Key management activities should include:

- Key generation
- Key distribution
- Secure key storage
- Identification of key custodians and associated requirements for dual access control
- Prevention of unauthorised substitution of keys
- Replacement of known or suspected compromised keys
- Key revocation, logging and auditing, and other key management related activities.

## How Thales Can Help Organisations Adhere to UIDAI's Aadhaar Data Vault Mandates

As outlined by UIDAI, merely building an Aadhaar Data Vault doesn't fulfil the mandated compliances.

For cohesively protecting the Aadhaar data, Tokenization must be used to disguise the original Aadhaar Numbers and the corresponding reference keys (along with the mapped Aadhaar data) should be encrypted. Furthermore, the encryption keys must be stored in HSM devices that are inherently designed to offer foolproof protection against intrusions and tampering.

Thales's extensive range of data protection solutions not only help organisations cohesively protect the Aadhaar data but also help them seamlessly comply with UIDAI's Aadhaar Data Vault mandates.

## CipherTrust Tokenization

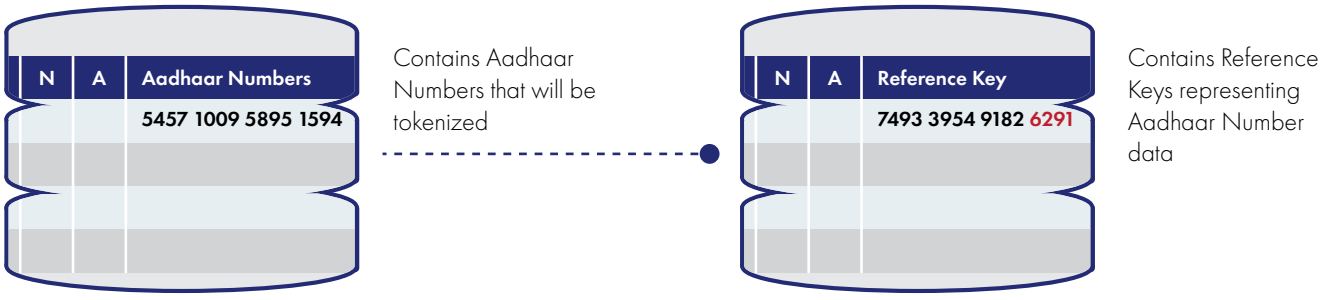
CipherTrust Tokenization dramatically reduces the cost and effort required to comply with security policies and regulatory mandates like UIDAI's Aadhaar Data Vault mandate while also making it simple to protect other sensitive data including personally identifiable information (PII) like the Aadhaar data.

It uses a format-preserving token with an irreversible option that can go up to a data length of 128K. With custom-defined formats and fixed masking, it offers a convenient workflow and a graphical interface. The result is an option for direct API requests from the servers with just a single line of code inserted into applications. It leverages CipherTrust Manager as a secure encryption key source.

The RESTful APIs in combination with centralised management consolidates all the data and stores it in an encrypted format. The unique and randomised tokens are linked to reference keys, the mapping for which is stored only in the Aadhaar Data Vault. Client authentication is needed by an application for any transmission of tokens, followed by comprehensive auditing and logging capabilities. The solution optimizes the regulatory processes bringing down the total cost of ownership (TCO) effectively.

CipherTrust Tokenization is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business.

### Application tables modification:




**Customer Original DB**

**Altered DB Post Tokenization**

### Tokenization added tables:


**Aadhaar Data Vault**
(In Audit Scope)

**CipherTrust Tokenization and CipherTrust Manager**

## Thales Luna HSMs

Thales Luna HSMs are a secure crypto foundation with the highest level of security there is for providing hardware root of trust to aadhaar encryption keys. The data is always protected in a tamper-resistant, intrusion-proof FIPS 140-2-validated device that secures sensitive information from unauthorised access.

In addition to a strong secure architecture, a keys in hardware approach, and superior performance, Luna HSMs also stand out from other HSMs through their integration with Thales Crypto Command Center that seamlessly allows reporting, partitioning, monitoring and alerting for granular-level access and authorisation controls.

Here's how Luna HSMs comply with UIDAI's Aadhaar Data Vault mandates:

- Encryption keys are protected by tamper resistant hardware that maintains the data integrity.
- The FIPS 140-2 Level 3-validated Luna HSMs safeguard the Aadhaar encryption keys.
- Broad API support brings in the power to use a combination of products and features.
- Auto logging and reporting takes care of the documentation and compliances.

With Thales Luna HSMs, a crypto-agile infrastructure balances security and performance to deliver strong authentication and role separation for all Aadhaar-related operations.

As all generation, management and storage of cryptography key materials are confined within the tamper-proof HSM, the chances of a data breach are significantly mitigated.

Luna HSMs comprehensively fulfil UIDAI's Aadhaar Data Vault compliances and help organisations cohesively protect and manage the Aadhaar data in a safe, secure, and reliable IT environment.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

**Contact us**

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

**> cpl.thalesgroup.com <**