# SOLUTION BRIEF

## Odisha Aadhaar Authentication Framework (OAAF)

### Introduction

Aadhaar is the unique identification number provided to every Indian by Unique Identification Authority of India (UIDAI). To implement the Aadhaar authentication at service delivery points in the state level an application namely Aadhaar Authentication Framework has been established in every state. IT department, Govt. of Odisha state as an entity called AUA (Authentication User Agency) developed an application called Odisha Aadhaar Authentication Framework (OAAF).

It has a centralized setup at the Odisha State Data Centre (OSDC) to cater to the needs of its various departments. While each of the line departments are able to authenticate data pertaining to their own department after following the UIDAI standards and guidelines, Aadhaar Authentication Framework offers the government to streamline their delivery mechanism under the welfare schemes, thereby ensuring transparency and efficiency.

Different departments involved in delivery of Aadhaar authentication can integrate themselves as Sub-AUA (Authentication user Agency) to use resident authentication services. As on date more than 16 Sub-AUAs are integrated with multiple schemes in OAAF.

### Solution Details

OAAF is providing three major services namely Authentication of the Aadhaar Numbers, Aadhaar eKYC and Aadhaar Data Vault.

**Authentication:** Authentication enables Aadhaar-holders to prove their identity and for confirming the resident's identity claim in order to provide services and give access to benefits either through Biometric Matching (Fingerprint Authentication & IRIS Authentication), Demographic Matching or One-Time-PIN (OTP) by Authentication User Agency.

**E-KYC:** The Aadhaar e-KYC service provides an instant, electronic, proof of identity and proof of address along with date of birth and gender. E-KYC may be performed at an agent/ service delivery location using biometric authentication, as well as remotely using an OTP.

**Aadhaar Data Vault:** Aadhaar Data Vault Solution provides the reference number against Aadhaar number to store in scheme databases. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault. All Sub-AUAs shall use this Reference Key instead of Aadhaar number in all systems where such reference key needs to be stored/mapped.

### Solution Key Features and Benefits

OAAF is effectively managing the resident data in a digitized, centralized way and in secured manner, thus enhancing Aadhaar security, leverage resident data in service delivery applications and incorporate Aadhaar Authentication into various applications.

- OAAF helps the state government in maintaining a lean database and ensures privacy of data.
- OAAF supports Secure Authentication using Registered Device (RD), Virtual ID (VID) which helpful for privacy protection introducing an encrypted Aadhaar format and helps in storing of UID token on UIDAI response.

- Aadhaar authentication requests are encrypted using document signer certificate which is stored using Thales Luna HSM.
- Aadhaar Data Vault containing Aadhaar number/data, and the referencing system kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.
- Aadhaar number and any connected data maintained on the Aadhaar Data Vault shall always be kept encrypted and access to it is strictly controlled only for authorized systems. Keys used for encryption are stored in Thales Luna HSM only.

## Integration with Thales LUNA HSM

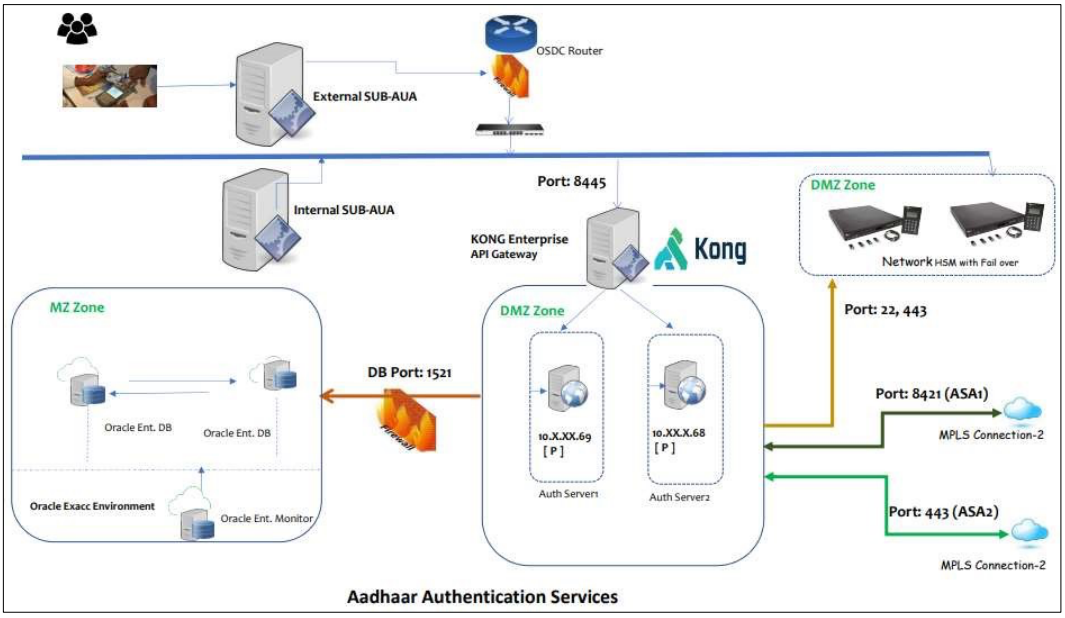
Thales Luna HSMs store, protect, and manage sensitive cryptographic keys in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure.

With above mentioned features and advantages of Thales Luna HSM, we integrated Luna HSM with two of our solutions. One is in authentication/ eKYC and another is Aadhaar data vault.

- Thales Luna HSM is configured in DMZ zone for high availability
- Digital certificates are imported into Luna HSM
- Luna client is installed into server for running within the application
- HSM physical connectivity is established for fetching certificate details through application programming
- Implemented the complete integrated solution to perform transactions through the respective application in conjunction with Luna HSM

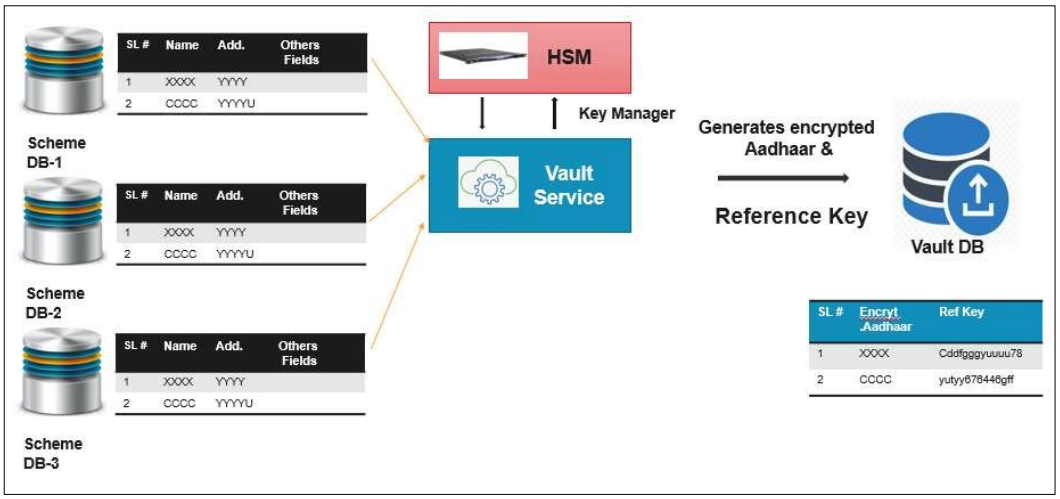
## Architecture Diagram

A. Authentication Architecture




*In the above diagram, Thales Luna HSM is used for storing digital signature certificate for authentication.*

B. Aadhaar Data Vault Architecture




In the above diagram, Thales Luna HSM used for storing digital signature certificate for encrypting Aadhaar numbers.

## About CSM Technologies

CSM Technologies Private Limited is a CMMi L-5 Dev 2.1 certified organization dedicated to leveraging technology to bring about transformative changes in the realm of governance, enterprises, and citizen well-being. Taking immense pride in being pioneers in the GovTech sector, the team at CSM Technologies harnesses the power of both established and emerging technologies to deliver solutions that significantly enhance governmental efficiency and life of citizens.

CSM Technologies as of date had successfully conceptualized and executed more than 1200 IT projects across various domains, including mining, education, transport, land allotment, infrastructure, Smart Cities, and more. CSM's suite of solutions brings in process efficiency and optimize the performance of the government through automation & digitization. This not only helps in transforming government-citizen relationships but enhances the confidence of the citizens in the government machinery. The comprehensive suite of services includes IT Consulting & Advisory, Digital Services, Application Development, Visualization & Analytics, Open-Source ERP, IT Infrastructure and Data Storage & Server Management, Network & Data Security, and Managed Services.