Securing UIDAI Unique Identification Numbers with Thales Data Protection Solutions

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.

The UIDs are intended to: eliminate duplication and fake identities; empower residents to authenticate anytime, anywhere; and provide an easy, cost–effective way for residents to verify their identity and authenticate to Aadhaar-linked applications. In return, the Government of India is able to collect valuable demographic data on its constituents.

Mandatory use of HSMs and Tokenization for UIDAI

Due to the fact that the UIDs contain Personally Identifiable Information (PII), the UIDAI has mandated that the private cryptographic keys used to digitally sign and authenticate the UIDs must be stored in a Hardware Security Module (HSM) as of August 2017, and used as follows:

- Store the private keys used for digital signing of Auth XML and decryption of electronic "know your customers" (e-KYC) data
- Authentication User Agencies (AUA) and Know Your Customers User Agencies (KUA) must digitally sign the authentication requests and / or they must be signed by the Authentication Service Agency (ASA) HSM
- To decrypt the e-KYC response data received from the UIDAI, the KUA must use its own HSM
- The HSM to be used for signing Auth XML as well as for e-KYC decryption should be FIPS 140-2 compliant

In addition to HSMs, the UIDAI has also mandated the use of tokenization – replacing sensitive data with a token that can be securely stored, processed and transmitted:

- Each Aadhaar number is represented by a reference key. Mapping of reference key and Aadhaar number through tokenization is to be maintained in a separate secure database "Aadhaar Data Vault".
- The Aadhaar number and any connected data stored in Aadhaar Data Vault must be encrypted. Keys for encryption must be stored in an HSM.

Benefits of Thales Luna HSMs

Easily conform to UIDAI mandates with Thales Luna HSMs – dedicated crypto processors that are specifically designed to securely manage, process, and store crypto keys. Ensure your data is safe from a cyber-attack by storing your private cryptography keys inside a hardened, tamper-resistant, FIPS-validated device. Without access to the keys, data is rendered useless. Your organization will benefit from our years of experience, and stringent product verification testing that certifies the security and integrity of our devices.

What makes our HSMs unique?

- **Keys always remain in tamper-resistant hardware** – protected at all times unlike alternative HSMs that store keys in software
- Secure your sensitive UID cryptographic keys in **our FIPS 140-2 Level 3-validated HSMs**
- Benefit from **high performance** to satisfy your UIDAI applications and meet service level agreements
- **Strong Authentication and Access** - application Private Keys remain secure from access in case of a breach
- **Flexibility** through broad API support as well as an unparalleled combination of products and features
- **Audit logging and reporting** – reduces audit and compliance

HSM or no HSM?

Storing UIDAI signing and encryption private keys on a HSM and following best practices ensures your keys, and ultimately your data, are secure from malicious attacks:

- Without access to your keys, encrypted data is useless and has no financial value
- Ensure that critical functions and processes such as key generation, storage, backup, and access control are secure, occurring within the safe confines of the hardware appliance
- Offload and accelerate UIDAI cryptographic operations to the dedicated, purpose-built, high-security cryptographic processor, eliminating bottlenecks and maximizing application performance for encryption, authentication and signing transactions
- Strictly control access to the HSM and keys through MofN authentication and a Pin Entry Device (PED)
- Delegate cryptographic separation and administration in order to keep keys secure and ensure that only authorized parties have access to the key, using strong separation of duties via a security officer per partition

To compare, keys in software are unprotected and vulnerable, prone to attack. Gaining access to the software also means access to the encryption keys, providing the ability to manipulate resident identification and collected data. Furthermore, processes such as digital signing consume over 80% of application server resources, resulting in slow authentication and frustration for residents.

Not all HSM are created equal

Thales takes a keys-in-hardware approach to managing and storing encryption keys, unlike other HSM solutions that store keys in software. With Luna HSMs, your UIDAI private keys are protected at all times in a hardware root of trust:

- Secure your sensitive UID cryptographic keys in our FIPS 140-2 Level 3–validated HSMs
- Store your private keys in a high-assurance vault to ensure they are safe from breach
- Keys never leave the HSM - applications communicate via a client with keys stored in the Luna HSM

About Thales KeySecure and Thales Tokenization

Thales Tokenization uses Format Preserving Tokenization (FPT) to preserve sensitive data's length and format in order to minimize the need to modify applications, databases, and legacy systems that will store, process, or transmit the associated token. Benefit from unlimited data type support, including numeric data with spaces or dashes such as the information found in UIDAI applications, and Aadhaar's. Tokenization also provides the ability to apply granular access controls to ensure only authorized users or applications can view tokenized data, and administrators can track access to tokens and protected data with comprehensive auditing and logging capabilities.

Tokenization relies on Thales KeySecure, a FIPS 140-2 up to Level 3 validated enterprise key manager (available as both a physical and virtual appliance), that provides centralized cryptographic processing, key and policy management.

This solution from Thales is compliant with PCI Tokenization Guidelines and VISA Tokenization Best Practices, and is ideal for organizations looking to significantly reduce regulatory scope, facilitate the annual audit process, and reduce total cost of ownership.

How can we help you become UIDAI compliant?

Contact Thales to learn how you can quickly meet UIDAI compliance mandates, bring trust and security to your UIDAI applications, and ensure Aadhaar are protected against duplication with FIPS-validated, tamper-resistant Luna HSMs, KeySecure, and Tokenization.

भारत सरकार
GOVERNMENT OF INDIA

सुखराजदीप सिंह
Sukhrajdeep Singh

जन्म वर्ष / Year of Birth : 1987
पुरुष / Male

2333 8823 0337

आधार — आम आदमी का अधिका

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.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com