Complying with UIDAI's Aadhaar number regulations

Entrust helps enterprises comply with key UIDAI requirements

- Maintain cryptographic keys in FIPS-certified HSMs
- Prevent unauthorized access to information facilities
- Improve compliance with E-KYC and Aadhaar Data Vault guidelines

SUMMARY

The Unique Identification Authority of India (UIDAI) was established under the provisions of India's 2016 Aadhaar Act. UIDAI is responsible for issuing unique identification numbers (UIDs), called Aadhaar, and providing Aadhaar cards to all residents of India. The 12-digit UIDs are generated after the UIDAI verifies the uniqueness of enrollees' demographic and biometric information; UIDAI must protect individuals' identity information and authentication records.

Entrust can help your organization comply with key elements required for Aadhaar.

Regulation and Entrust Solution

The **Compendium of Regulations, Circulars & Guidelines for (Authentication User Agency (AUA)/E-KYC User Agency (KUA), Authentication Service Agency (ASA) and Biometric Device Provider) outlines the information security policy documents specifying the scope and requirements for the UIDAI. The chart that follows matches specific security controls excerpted from the regulatory compendium to Entrust security offerings.**

Complying with UIDAI's Aadhaar number regulations

Aadhaar Security Control	Entrust Security Coverage
User access control **Access Control** Only authorized individuals shall be provided access to information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing UIDAI information.	**nShield HSMs** nShield HSMs can help you create high-assurance systems to authenticate users and devices using enterprise systems, limiting access to only authorized entities.
Encryption key management **Cryptography** Key management activities shall be performed by all AUAs / KUAs to protect the keys throughout their lifecycle. The activities shall address the following aspects of key management, including; a) Key generation b) Key distribution c) Secure key storage d) Key custodians and requirements for dual Control e) Prevention of unauthorized substitution of keys f) Replacement of known or suspected compromised keys g) Key revocation and logging and auditing of key management related activities	**nShield HSMs** Entrust partners with leading technology providers to deliver high assurance, highly scalable centralized key management that protects keys throughout their lifecycle. The nShield HSM provides strong key generation through its high entropy random number generator and the hardened environment provides FIPS and Common Criteria certified protection of the underpinning encryption keys and the security of the entire system. nShield cloud Bring Your Own Key allows you to use your on-premises HSM to generate and manage keys that you bring to your public applications.
Mandatory use of HSMs 1. To further enhance the security of Aadhaar authentication eco-system, under Regulations 14(n) and 19 (o) of Aadhaar (authentication) Regulations, 2016, it is hereby decided to mandatorily use Hardware based Security Module (HSM) for digital signing of Auth XML and decryption of e-KYC data. 2. For digital signing of Auth XML, Authentication request shall be digitally signed by the requesting entity (AUA/KUA) and/or by the ASA using HSM, as per the mutual agreement between them. However, to decrypt the e-KYC response data received from UIDAI, the KUA shall necessarily 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. 3. Therefore, all AUA/KUA/ASA shall ensure the implementation of HSM in Aadhaar authentication services in aforesaid manner before 31st August, 2017 and submit the compliance report. Any non-compliance in this regard will amount to violation of Aadhaar Act 2016, its Regulations and AUA / ASA Agreement (including schedule of financial disincentives) making the concerned liable for appropriate penal action as provided therein which shall be in addition to any other legal action as per relevant laws.	**nShield HSMs** nShield® HSMs provide a FIPS 140-2 Level 3 compliant environment for secure digital signing, cryptographic processing, key protection and more.

Complying with UIDAI's Aadhaar number regulations

Aadhaar Security Control	Entrust Security Coverage
The use of FIPs 140-2 certified HSMs for cryptographic key protection The course of action to implement the process by all AUAs/KUAs/Sub-AUAs and other entities is hereby outlined below: The Aadhaar number and any connected data maintained on the Aadhaar Data Vault shall always be kept encrypted and access to it strictly controlled only for authorized systems. Keys for encryption are to be stored in HSM devices only.	**nShield HSMs** nShield HSMs provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption and more. Certified at FIPS 140-2 Levels 2 and 3, nShield HSMs support a variety of deployment scenarios including nShield-as-a-service. nShield and Solo HSMs also provide a secure environment for running sensitive applications. nShield hardware security modules protect enterprise and cloud-hosted Microsoft SQL Server and Oracle Databases. nShield HSMs complement Oracle Database native TDE by centrally storing and managing Oracle Database encryption keys. As a part of the Oracle Advanced Security TDE two-tier key architecture, Oracle Database uses master encryption key (MEKs) to encrypt the database encryption keys (DEKs), which are used to encrypt columns and tablespaces within the databases. nShield HSMs interface with the Oracle Wallet and Oracle Key Vault to protect and manage these MEKs within a secure FIPS-certified boundary.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com