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 Tokenization for UIDAI

Due to the fact that the UIDs contain Personally Identifiable Information (PII), the UIDAI has mandated replacing sensitive data with a surrogate value – or reference key – that can be securely stored, processed and transmitted: UIDAI requires:

> 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.

What the UIDAI refers to as ‘reference keys’ many would term ‘tokens’. Gemalto’s SafeNet Tokenization solution assigns Aadhaar numbers completely random surrogate values – or tokens – in an encrypted database. Applications needing the Aadhaar number instead receive the token for its purposes. With SafeNet Tokenization solutions, the Aadhaar number never leaves the encrypted database. And, relying on SafeNet KeySecure, Gemalto’s enterprise key management platform, organizations can store all necessary encryption keys in a secure appliance per UIDAI’s obligations.

About SafeNet Tokenization and SafeNet KeySecure

SafeNet Tokenization secures Aadhaar numbers by using surrogate values – or tokens – that reside in a special encrypted database. Tokens maintain the length and format of the sensitive data they replace in order to minimize the need to modify applications, databases, and legacy systems that would store, process, or transmit this information. With SafeNet Tokenization solutions, organizations benefit from unlimited data type support, including numeric data with spaces or dashes such as the information found in UIDAI applications.

SafeNet Tokenization Benefits

Ensure Compliance:
> Replace Aadhaar numbers with appropriate reference keys (tokens), record usage and access in administrative logs, and control access to the token vault using robust access controls, all per UIDAI mandates.

Centralize and Streamline Data Security:
> Unify administration and extend data protection to all layers of the technology stack with SafeNet KeySecure and the full portfolio of SafeNet encryption solutions

Leverage the Cloud Securely:
> Maintain complete ownership and control of your data and keys in virtual, public cloud, and hybrid environments

Speed Time to Deployment:
> Simplify integration and ongoing processes by leveraging SafeNet Tokenization’s web services, APIs, and bulk tokenization capabilities
And, its granular access control functionality ensures that only authorized users or applications can view tokenized Aadhaar numbers. For robust security and for more easily demonstrating UIDAI compliance, administrators can track access to tokens and the corresponding Aadhaar numbers with comprehensive auditing and logging capabilities.

SafeNet Tokenization relies on SafeNet KeySecure, a FIPS 140-2 up to Level 3 validated enterprise key manager (available as both a physical and virtual appliance) to provide centralized cryptographic processing, key and policy management. All communications between the SafeNet token vault, SafeNet KeySecure and applications using tokens are done over secure channels per the UIDAI requirement.

**Mandatory Use of Hardware Security Modules (HSM) for UIDAI**

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

HSMs are dedicated cryptographic processors specifically designed to securely manage, process, and store cryptographic keys. SafeNet Luna HSMs help organizations easily conform to UIDAI mandates and ensure data is safe from cyber-attacks by storing private cryptographic keys inside a hardened, tamper-resistant, FIPS 140-2 Level 3-validated device at all times. Without access to the keys, data is rendered useless to hackers. Benefit from Gemalto’s experience and stringent product verification testing that certifies the security and integrity of our devices.

**Conclusion**

Contact Gemalto to learn how to quickly meet UIDAI compliance mandates, bring trust and security to UIDAI applications, and ensure Aadhaar are protected against duplication. In addition to UIDAI requirements, Gemalto’s portfolio of SafeNet solutions is compliant with PCI Tokenization Guidelines, VISA Tokenization Best Practices, the European Union’s General Data Protection Regulation (GDPR) and is ideal for organizations looking to significantly reduce their regulatory scope, facilitate the annual audit process, and reduce total cost of ownership.

For more information visit: [https://safenet.gemalto.com/](https://safenet.gemalto.com/)

**About Gemalto’s SafeNet Identity and Data Protection Solutions**

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core.

Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

**Contact Us:** For all office locations and contact information, please visit safenet.gemalto.com

**Follow Us:** blog.gemalto.com/security