cpl.thalesgroup.com

THALES
Building a future we can all trust

Complying with UIDAI's AADHAAR Number Regulations

Compliance Brief

Introduction

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.

Thales can help your organization comply with many of the regulations and mandates required for Aadhaar.

Regulation and Thales Solution

The following standards are excerpted from the "UIDAI Information Security Policy – UIDAI External Ecosystem – Authentication User Agency/ KYC User Agency" section of UIADAI's 30 April 2018 update of its Compendium of Regulations, Circulars & Guidelines for (Authentication User Agency (AUA)/E-KYC User Agency (KUA), Authentication Service Agency (ASA) and Biometric Device Provider) [The Compendium]. See the next page for many elements of the regulation and how Thales can help you comply with them.

Thales helps enterprises comply with key UIDAI requirements

- Control access to demographic and biometric data
- Encrypt citizens' sensitive information
- Monitor and log data base access to identify and stop attacks
- Create format-preserved "Reference Keys" for business use outside the Aadhaar Data Vault by tokenizing Aadhaar numbers

AADHAAR SECURITY CONTROL	THALES COVERAGE
USER ACCESS CONTROL	**DATA SECURITY PLATFORM PRODUCTS**
SECTION 2 : Circulars, Guidelines with IS UIDAI Information Security Policy – AUA/KUA Part 2 – Information Security Policy for Authentication User Agencies (AUAs)/KYC User Agencies **Article 2.6 Access Control** 1. 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	CipherTrust Data Security Platform products include or support data-at-rest access controls as well as enforcing those controls with encryption and key management capabilities. **CipherTrust Transparent Encryption** – Provides policy-based, system-level, access controls at the file and volume level for system level to encrypted data. These controls can be applied to users and groups from systems, LDAP/ Active Directory, Hadoop, and containers and can include protection against root and other privileged user access. Controls can be applied wherever data is stored – in local data centers, hosted environments, and private or public Infrastructure-as-a-Service (IaaS) cloud implementations. **CipherTrust Database Protection** – Provides transparent column-level encryption of structured, sensitive data residing in databases, such as credit card, social security numbers, national ID numbers, passwords, and email addresses. **CipherTrust Tokenization with Dynamic Data Masking** – Enables access control to sensitive data stored within files or databases using format preserving or random tokenization. Includes the capability to dynamically masks portions of Aadhaar numbers by role typically used by call center and similar applications. **CipherTrust Application Data Protection** – Designed to make it easy to add data-at-rest encryption into applications, it enables developers to build access control capabilities into their applications. Eliminates system level access to data that it encrypts for protection against privileged user and system level internal and external threats. **CipherTrust Enterprise Key Management** – Includes TDE masker key management for Oracle and Microsoft SQL databases – enabling database level access control to encrypted UIDAI data. Also eliminates system level access to encrypted data within the database. Also manages keys for KMIP compliant devices, eliminating access to encrypted UIDAI data if devices are lost, stolen or improperly retired. **CipherTrust Cloud Key Manager** – Eliminates cloud provider access to UIDAI data sets used within their environments by controlling and managing encryption keys used to protect data in the cloud. Environments supported include AWS compute, Azure Compute, IBM Cloud, Microsoft Office 365, SalesForce, Google Cloud and others. **CipherTrust Protection for Teradata Database** – Secures UIDAI data stored within Teradata database environments from external access and enforces granular access controls within the database that can prevent administrative or unauthorized access to UIDAI data.

AADHAAR SECURITY CONTROL	THALES COVERAGE
ENCRYPTION OF DATA	**CIPHERTRUST TRANSPARENT ENCRYPTION** **CIPHERTRUST APPLICATION DATA PROTECTION**
SECTION 2 : Circulars, Guidelines with IS UIDAI Information Security Policy – AUA/KUA Part 2 – Information Security Policy for Authentication User Agencies (AUAs)/KYC User Agencies **Article 2.8 Cryptography** 2. The PID shall be encrypted during transit and flow within the AUA / KUA ecosystem and while sharing this information with ASAs; 3. The encrypted PID block should not be stored unless in case of buffered authentication for not more than 24 hours after which it should be deleted from the local systems;	Definition: "PID Block" means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication. Article 2.8 – (2.) Requires that this information be encrypted in transit or where used, with (3.) requiring that it not be stored for more than 24 hours. I.e. – even temporary storage will require that the PID be encrypted. Applicable CipherTrust Data Security Platform products include: **CipherTrust Transparent Encryption** – Encrypt files or volumes containing PID data at the file system or volume level. Provides policy-based, system-level, encryption (with access controls as described above) within systems. Use to encrypt data stores that include PID data. Encryption can be applied wherever data is stored – In local data centers, hosted environments, and private or public Infrastructure as a Service (IaaS) cloud implementations. It can be used with Linux, AIX and Windows file systems or volumes, database file or volumes, big data environments, containers or linked cloud storage environments. **CipherTrust Application Data Protection** – Easily encrypt files or database fields that include PID data using a local agent on systems or via RESTful APIs. Can be deployed across data centers, cloud environments, big data implementations and containers.
ENCRYPTION KEY MANAGEMENT	**CIPHERTRUST MANAGER** **CIPHERTRUST ENTERPRISE KEY MANAGEMENT** **CIPHERTRUST CLOUD KEY MANAGER**
SECTION 2 : Circulars, Guidelines with IS UIDAI Information Security Policy – AUA/KUA Part 2 – Information Security Policy for Authentication User Agencies (AUAs)/KYC User Agencies **Article 2.8 Cryptography** 6. 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.	**CipherTrust Data Security Manager** – The CipherTrust provides secure encryption key and policy management for all CipherTrust Data Security Platform Products that meets these requirements. **CipherTrust Enterprise Key Management** also meets these requirements for secure encryption key management for Oracle and Microsoft SQL databases using TDE encryption, as well as for KMIP compatible devices **CipherTrust Cloud Key Manager** meets these requirements for encryption key management for cloud environments that includes Microsoft Azure, Google Compute, Amazon AWS Infrastructure-as-a-Service offerings, as well as Microsoft Office 365, IBM Cloud and Salesforce.

AADHAAR SECURITY CONTROL	THALES COVERAGE
REQUIREMENTS WHEN STORING AADHAAR NUMBERS IN DATABASES	**CIPHERTRUST DATA SECURITY PLATFORM PRODUCTS**
SECTION 3 : Other Circulars, Guidelines etc. **3.14 DOs & DON'Ts FOR AADHAAR USER AGENCIES/DEPARTMENTS** 7. If agency is storing Aadhaar number in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using HSMs. If simple spreadsheets are used, it must be password protected and securely stored. 8. Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.	CipherTrust Data Security Platform products provide encryption and secure encryption key management for databases: **CipherTrust Transparent Encryption** – Encrypts database volumes or files and controls access by policy **CipherTrust Database Protection** – Provides transparent column-level encryption of structured, sensitive data residing in databases, such as credit card, social security numbers, national ID numbers, passwords, and email addresses. **CipherTrust Application Data Protection** – Provides libraries and RESTful APIs that enable developers to easily encrypt data such as Aadhaar numbers stored in databases. Acts as the enforcement layer for access controls set by application and database rules. **CipherTrust Tokenization with Dynamic Data Masking** – offers application-level tokenization services in two convenient solutions to replace sensitive data such as Aadhaar numbers with tokens: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets—whether they reside in the data center, big data environments or the cloud. **CipherTrust Enterprise Key Management** – Enables secure, compliant management of TDE encryption keys for Oracle and Microsoft SQL databases, enabling field and column level encryption of Aadhaar numbers, and database level access controls **CipherTrust Manager** – Provides secure encryption key and policy management for CipherTrust Data Security Platform products. The CipherTrust Manager can be purchased with an internal HSM to protect encryption keys with a secure root of trust within the device, or can use an external Thales Luna HSM for a secure root of trust.
FAQS FOR THE AADHAAR VAULT AND REFERENCE KEYS	**CIPHERTRUST DATA SECURITY MANAGER**
SECTION 3 : Other Circulars, Guidelines etc. **3.14 Frequently Asked Questions (FAQs) for Aadhaar vault and Reference Keys** 10. Can existing HSMs be used for storing the encryption keys? Agencies may use the existing HSMs. HSMs used to store the keys for encryption of Aadhaar data vault cannot be shared with any other agency/legal entity. Security of the partitions storing Aadhaar data vault keys need to be ensured by the agency.	The **CipherTrust Manager** – Provides secure encryption key and policy management for CipherTrust Data Security Platform products. The CipherTrust Manager can be purchased with an internal Thales Luna HSM to protect encryption keys with a secure root of trust within the device, or can use an external Thales Luna HSM for a secure root of trust.

AADHAAR SECURITY CONTROL	THALES COVERAGE
DATABASE ACCESS LOGGING	**CIPHERTRUST SECURITY INTELLIGENCE LOGS**
2.10 Operations Security 12. AUAs/KUAs shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring; 13. Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only.	The CipherTrust Transparent Encryption Security Intelligence Logs enables organizations to identify unauthorized access attempts and to build baselines of authorized user access patterns. CipherTrust Security Intelligence integrates with leading security information and event management (SIEM) systems that make this information actionable. The solution allows immediate automated escalation and response to unauthorized access attempts, and all the data needed to build behavioral patterns required for identification of suspicious use by authorized users, as well as training opportunities.

The following excerpts are from Circular 11020/205/2017 in The Compendium:

TOKENIZATION OF AADHAAR NUMBERS	CIPHERTRUST TOKENIZATION
In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all AUAs/KUAs/Sub-AUAs and other entities that are collecting and storing the Aadhaar number for specific purposes under the Aadhaar Act 2016, shall start using Reference Keys mapped to Aadhaar numbers through tokenization in all systems.	CipherTrust Tokenization dramatically reduces the cost and effort required to comply with security policies and regulatory mandates, such as Aadhaar. The solution offers application-level tokenization services in two convenient solutions to replace sensitive data such as Aadhaar numbers with tokens: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets—whether they reside in the data center, big data environments or the cloud.

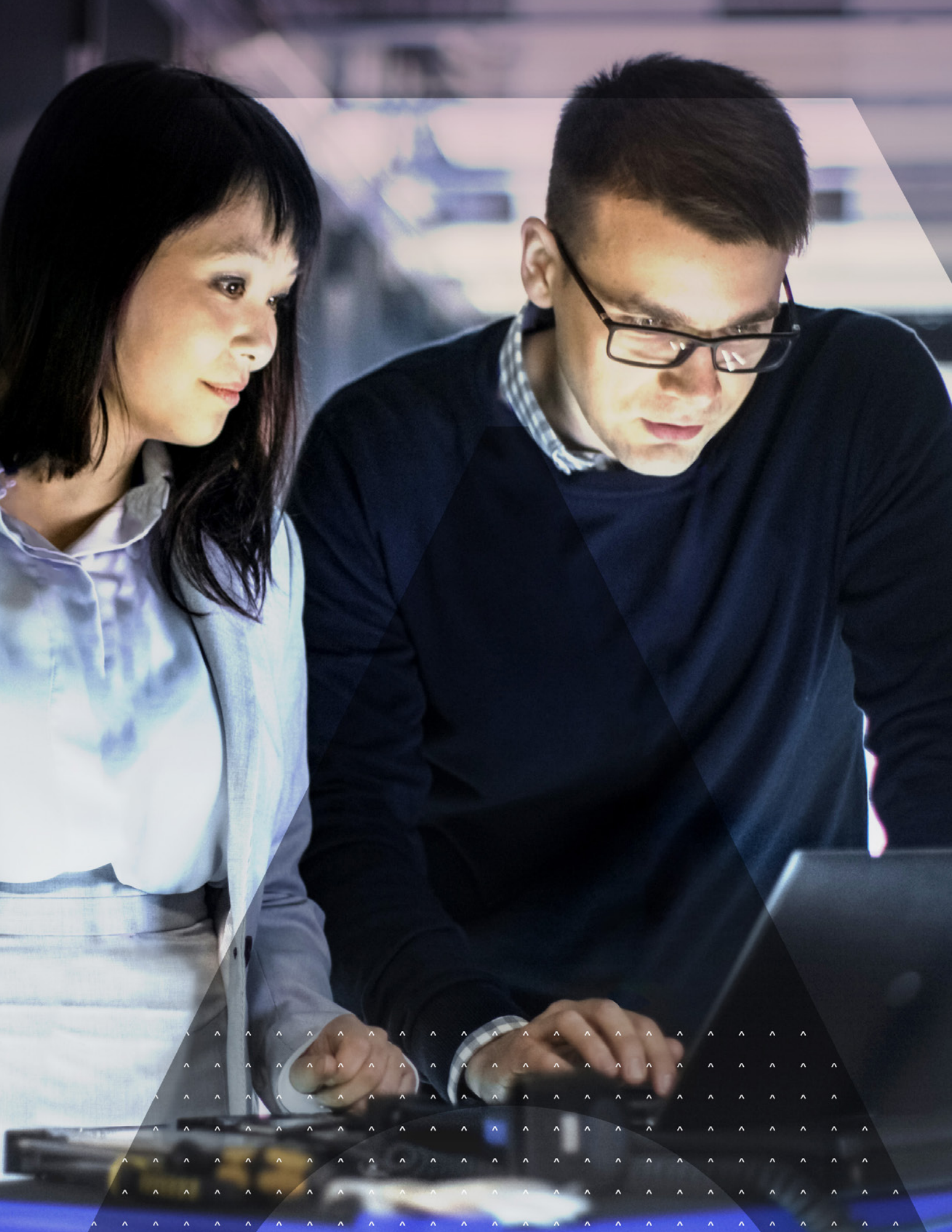
For More Information

For more detailed information on these products, please visit cpl.thalesgroup.com.

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 <