Trusted Cyber Technologies

THALES

NIST 800-57 Recommendations for Key Management Requirements Analysis

White Paper

ABSTRACT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57, Recommendations for Key Management Part 1 (Rev 5) provides guidance for cryptographic key management for U.S. Federal Government agencies. Part 1 of the publication outlines best practices for the management of cryptographic keys and discusses key management issues that must be addressed with using cryptography.

Importance of Securing Cryptographic Keys

The security of cryptographic processes is dependent on the security of the cryptographic keys used to encrypt the data. If the keys used to encrypt data are stolen with the encrypted data, the data is not secure because it can be deciphered and read in plain text.

NIST emphasizes the importance of protecting cryptographic keys in the publication, "The proper management of cryptographic keys is essential to the effective use of cryptography for security. Poor key management may easily compromise strong algorithms."[1] NIST states that:

> *Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of cryptographic mechanisms and protocols associated with the keys, and the protection provided to the keys. Secret and private keys need to be protected against unauthorized disclosure, and all keys need to be protected against modification.* [2]

For encryption to successfully secure sensitive data, the cryptographic keys themselves must be secured, managed and controlled by your organization and not a third-party or cloud provider. As agencies deploy ever-increasing numbers of siloed encryption solutions, they find themselves managing inconsistent policies, different levels of protection, and escalating costs.

The simplest path through this maze is to transition to a centralized key management model. Encryption key management involves administering the full lifecycle of cryptographic keys and protecting them from loss or misuse. Keys have a life cycle: They're created, live useful lives, and are retired. Key lifecycle management includes generating, using, storing, distributing, archiving, and deleting keys.

Thales Trusted Cyber Technologies' (TCT) Enterprise Key Management

Thales TCT's CipherTrust Manager is an enterprise key management platform that enables agencies to centrally manage encryption keys. It simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion.It provides role-based access control to keys and policies, multi-tenancy support, and robust auditing and reporting of all key management and encryption operations.

CipherTrust Manager is available in both virtual and physical form-factors that can use FIPS 140-2 validated appliances for securely storing master keys with an elevated root of trust. These appliances can be deployed on-premises as well as in private or public cloud infrastructures.

Benefits

Unified Management Console

CipherTrust Manager provides a single pane of glass for discovering and classifying sensitive data integrated with a comprehensive set of data protection connectors to encrypt or tokenize data to reduce business risk and satisfy compliance regulations. It streamlines provisioning of connector licenses through a new customer facing licensing portal and provides better visibility and control of licenses in use.

Centralized Key Management and Access Control

It offers centralized key lifecycle, certificate and policy management with role-based access control and provides full audit log review. It authenticates and authorizes administrators and key users using existing AD and LDAP credentials.

Cloud Friendly Deployment Options

CipherTrust Manager offers several options to securely migrate applications to multiple cloud environments. It offers support for AWS, Azure, Google Cloud, VMware, HyperV, Oracle VM and more. In addition, CipherTrust Cloud Key Manager supports bring your own key (BYOK) across multiple cloud infrastructures and SaaS applications.

Developer Friendly APIs

CipherTrust Manager offers new REST interfaces, in addition to KMIP and NAE-XML APIs, for developers to simplify deployment of applications integrated with key management capabilities and automate development and testing of administrative functions.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

Improved Monitoring and Alerting

It includes tracking of all administrator access, encryption key state and policy changes in multiple log formats (RFC-5424, CEF, and LEEF) for easy integration with SIEM tools. In addition, customers can generate pre-configured and customizable email alerts (SNMP v1, v2c, v3).

Hybrid High-Availability Clustering

It offers a choice of clustering CipherTrust Manager physical appliances (k470, k570) and a virtual appliances (k170v, k470v) for high-availability environments to ensure optimum processing regardless of the workload location (data center or cloud).

Robust Separation of Duties and Multitenancy Support

CipherTrust Manager can enforce strong separation of duties by requiring the assignment of key and policy management privileges to one or more data security administrators for different departments within a large enterprise. It provides capabilities to create multiple domains to support large enterprises with distributed locations.

FIPS 140-2 Compliant

CipherTrust Manager provides several options to integrate with a FIPS 140-2 validated HSMs as a secure root of trust for better key entropy

- Built-in HSM crypto accelerator card on a CipherTrust Manager k570 appliance
- Network attached Luna HSM with HA clustering
- Luna Cloud HSM on Data Protection on Demand and other cloud HSMs like AWS CloudHSM, Azure Dedicated HSM, and IBM Cloud HSM

NIST SP 800-57 Requirements Mapping

Focusing on the capabilities needed to meet the requirements outlined in NIST SP 800-57, the following table provides details on Thales TCT's CipherTrust Manager.

NIST 800-57 Reference	Requirement	Requirement Met	Thales TCT CipherTrust Manager
6	**Protection Requirements for Key Information**		
6.1	Protection and Assurance Requirements	✓	CipherTrust Manager is available in both virtual and physical form factors with varying FIPS 140-2 certifications. The virtual appliances can utilize one of several different network-accessible HSM's for a FIPS 140-2 Level 3 root of trust and can be deployed on-premises as well as in private or public cloud infrastructures. For added security, the disk of the CipherTrust Manager appliance can be fully encrypted. Encryption can either be initiated when an instance is first launched, or on an already launched instance.
6.1.1	Summary of Protection and Assurance Requirements for Cryptographic Keys	✓	
6.1.2	Summary of Protection Requirements for Other Related Information	✓	
6.2	Protection Mechanisms	✓	CipherTrust Manager is available in both virtual and physical form factors with varying FIPS 140-2 certifications, the disk of the appliance can be fully encrypted. High availability provides an Active/Active clustered configuration with real-time replication of keys, policies, and configuration information across multiple appliances - enabling complete disaster recovery and business continuity. CipherTrust Manager supports a wide range of open standard cryptographic interfaces, including PKCS #11, JCE, and .NET. In addition, it also supports the Key Management Interoperability Protocol (KMIP). SafeNet's REST interface can be used to develop custom software utilizing the enterprise key management functionality of the CipherTrust Manager. (continued...)
6.2.1	Protection Mechanisms for Key Information in Transit	✓	
6.2.1.1	Availability	✓	
6.2.1.2	Integrity	✓	
6.2.1.3	Confidentiality	✓	
6.2.1.4	Association with Usage or Application	✓	
6.2.1.5	Association with Other Entities	✓	
6.2.1.6	Association with Other Related Key Information	✓	

NIST 800-57 Reference	Requirement	Requirement Met	Thales TCT CipherTrust Manager
6.2.2	Protection Mechanisms for Key Information in Storage	✓	CipherTrust Manager offers a range of robust security features: • Granular Attribute Based Access Control (ABAC) authorization capabilities > • Secure key distribution through support of SSL • Secure storage of key encryption keys on a SafeNet Luna Network HSM CipherTrust Manager, when used to provide encryption with CipherTrust Transparent Encryption (CTE) AES 256 encryption keys utilized are passed through an encrypted wrapper. The Administrator Web Interface of CipherTrust Manager is accessed through HTTPS. CipherTrust Transparent Encryption Agent-to-CipherTrust Manager communication is accomplished through the use of ephemeral ports. This provides an additional layer of encryption key protection, reducing risk. Keys versioned in CipherTrust Manager maintain a single set of key metadata but contains multiple sets of key data. Each set of key data belongs to a unique version of the key.
6.2.2.1	Availability	✓	
6.2.2.2	Integrity	✓	
6.2.2.3	Confidentiality	✓	
6.2.2.4	Association with Usage or Application	✓	
6.2.2.5	Association with the Other Entities	✓	
6.2.2.6	Association with Other Related Key Information	✓	
6.2.3	Metadata for Keys	✓	
7	**Key States and Transitions**		
7.1	Pre-activation State	✓	CipherTrust Manager, which centralizes keys, management and policies for all CipherTrust Data Security Platform products. Built on an extensible microservices architecture, CipherTrust Manager simplifies key lifecycle management including activities such as generation, backup and restore, deactivation and deletion. Role-based access to keys and policies, multi-tenancy support, and robust auditing and reporting of key usage and operational changes are additional core features of the product.
7.2	Active State	✓	
7.3	Suspended State	✓	
7.4	Deactivated State	✓	
7.5	Compromised State	✓	
7.6	Destroyed State	✓	
8	**Key-Management Phases and Functions**		
8.1	Pre-operational Phase	✓	The CipherTrust Data Security Platform provides security functions on the CipherTrust Manager that are isolated from normal operation and include domain creation, key creation, host creation, and audit-only. • If more than one domain is deployed, domain administrators and users are separated by domain. Administrators have the option of using different encryption algorithms and key lengths to provide even more separation. Encryption algorithms for each domain include AES 128 and 256. • Encrypted communications between CipherTrust Manager and agent is selectable. • CTE uses REST API for communicating over TLS 1.2 channel with CM. There is secure transmission control between the CipherTrust Manager, the daemon running on the host, and the SecFS portion that sits in the host's kernel space. The CipherTrust Manager creates a public/private key pair, generates a Certificate Signing Request (CSR), which generates a certificate authority certificate that is stored in the CipherTrust Manager database. (continued...)
8.1.1	Entity Registration Function	✓	
8.1.2	System Initialization Function	✓	
8.1.3	Initialization Function	✓	
8.1.4	Keying-Material Installation Function	✓	
8.1.5	Key Establishment Function	✓	
8.1.5.1	Generation and Distribution of Asymmetric Key Pairs	✓	
8.1.5.1.1	Distribution of Public Keys	✓	
8.1.5.1.1.1	Distribution of a Trust Anchor's Public Key in a PKI	✓	
8.1.5.1.1.2	Submission to a Registration Authority or Certification Authority	✓	
8.1.5.1.1.3	General Distribution of Static Public Keys	✓	
8.1.5.1.2	Distribution of Ephemeral Public Keys	✓	

NIST 800-57 Reference	Requirement	Requirement Met	Thales TCT CipherTrust Manager
8.1.5.1.3	Distribution of Centrally Generated Key Pairs	✓	The user space portion of the CipherTrust agent creates a public/private key pair. The public key is used to create a CSR for the host, and is sent back to the CipherTrust Manager, where the request is signed, sent back to the host, and creates a "blueprint" of the host, along with the certificate. The kernel space portion also creates an asymmetric key pair and follows the same certificate creation process in order to send the kernel space public key to the CipherTrust Manager.
8.1.5.2	Generation and Distribution of Symmetric Keys	✓	
8.1.5.2.1	Key Generation	✓	
8.1.5.2.2	Key Distribution	✓	
8.1.5.2.2.1	Manual Key Distribution	✓	
8.1.5.2.2.2	Automated Key Distribution/Key Transport/Key Wrapping	✓	
8.1.5.2.3	Key Agreement	✓	
8.1.5.3	Generation and Distribution of Other Keying Material	✓	Keys are passed between the CipherTrust Manager and the host by generating a one-time AES256 random key on the CipherTrust Manager. The desired encryption keys are encrypted using the random key. The random key password is encrypted using the kernel space public key. The entire payload is sent to the host system, where the kernel space private key decrypt the random key and password. The random key then decrypts the desired encryption keys, and those keys are applied to the file/directory/executable that is to be encrypted.
8.1.5.3.1	Domain Parameters		
8.1.5.3.2	Initialization Vectors	✓	
8.1.5.3.3	Shared Secrets	✓	
8.1.5.3.4	RBG Seeds	✓	
8.1.5.3.5	Other Public and Secret Information	✓	
8.1.5.3.6	Intermediate Results	✓	
8.1.5.3.7	Random Bits/Numbers	✓	
8.1.5.3.8	Passwords	✓	
8.1.6	Key Registration Function	✓	
8.2	Operational Phase	✓	Thales CipherTrust Manager offers capabilities for managing cryptographic keys across their lifecycle, including key generation, key import and export, and key rotation. Keys can be symmetric or asymmetric, variable sizes, and can be constrained to particular usages. With the CipherTrust Manager, all cryptographic keys are stored in a centralized, hardened appliance to simplify administration while ensuring tight security for the broadest array of data types. Active/Active clustering for the high availability can be configured. This provides high assurance deployments ensuring 24x7 uptime to support key management and data encryption requirements.
8.2.1	Normal Operational Storage Function	✓	
8.2.1.1	Cryptographic Module Storage	✓	
8.2.1.2	Immediately Accessible Storage Media	✓	
8.2.2	Continuity of Operations Function	✓	
8.2.2.1	Backup Storage	✓	CipherTrust Manager uses backup keys to encrypt a backup. The admin can generate a brand new backup key or point to an existing key when creating a backup. Backup keys are stored encrypted inside CipherTrust Manager by a secret from a security service. The backup includes a dump of db values, such as user keys, which are already wrapped using the key hierarchy illustrated above. The final backup file additionally gets encrypted using the selected backup key.
8.2.2.2	Key Recovery Function	✓	CipherTrust Manager, which centralizes keys, includes activities such as generation, backup and restore, deactivation and deletion. There are versioned backups and archives of keys. With key versioning management, CipherTrust Live Data Transformation ensures efficient backup and archive recovery to enable more immediate access. In a data recovery operation, archived encryption keys, recovered from the CipherTrust Manager, are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys.
8.2.3	Key Change Function	✓	
8.2.3.1	Re-keying	✓	
8.2.3.2	Key Update Function	✓	
8.2.4	Key Derivation Methods	✓	
8.3	Post-Operational Phase	✓	
8.3.1	Key Archive and Key Recovery Functions	✓	

NIST 800-57 Reference	Requirement	Requirement Met	Thales TCT CipherTrust Manager
8.3.2	Entity De-registration Function	✓	All clients with supported product installations (for example, ProtectFile, ProtectV, and CTE) can be managed on the CipherTrust Manager. A CipherTrust Manager Administrator can register clients (except ProtectFile clients) with the CipherTrust Manager, view registered clients, view and modify details, revoke registrations, and delete clients when they are no longer needed. As soon as a client is deleted from the CipherTrust Manager, all communication between the CipherTrust Manager and the client will stop immediately.
8.3.3	Key De-registration Function	✓	Within CipherTrust Manager there is a Key Admins group. Key Administrators have permissions to managing keys on the system. They can: • create or modify their own keys • perform key management operations on keys created by all users on the system There is a System Defined Group named "CTE Admins". Users within the "CTE Admins" group are CTE Administrators. Only users of the "CTE Admins" group can delete CTE keys. Depending on the Key Management usecase a specified admin within CipherTrust Manager will be able be to manage keys or delete keys that are not in use.
8.3.4	Key Destruction Function	✓	
8.3.5	Key Revocation Function	✓	
8.4	Destroyed Phase	✓	
9	**Additional Considerations**		
9.1	Access Control and Identity Authentication	✓	Through the use of kernel level agents providing AES-256 Encryption, the CipherTrust Manager exceeds and augments current access control solutions at the file, directory, drive, or target level at the Operating System and provides Least Privilege. In addition, only authorized admins and clients can access/communicate with CipherTrust Manager.
9.2	Inventory Management	✓	CipherTrust Manager, which centralizes keys, management and policies for all CipherTrust Data Security Platform products. Built on an extensible microservices architecture, CipherTrust Manager simplifies key lifecycle management including activities such as generation, backup and restore, deactivation and deletion.
9.2.1	Key Inventories	✓	
9.2.2	Certificate Inventories	✓	
9.3	Accountability	✓	
9.4	Audit	✓	CipherTrust Manager, which centralizes keys, management and policies for all CipherTrust Data Security Platform products. Built on an extensible microservices architecture, CipherTrust Manager simplifies key lifecycle management including activities such as generation, backup and restore, deactivation and deletion.
9.5	Key-Management System Survivability	✓	CipherTrust Manager appliances in a clustered configuration with real-time replication of keys, policies, and configuration information across multiple appliances - enabling complete disaster recovery and business continuity. For large distributed enterprises that use multiple encryption solutions, keys can be centrally managed without making any perceptible impact on system performance

NIST 800-57 Reference	Requirement	Requirement Met	Thales TCT CipherTrust Manager
9.5.1	Backed Up and Archived Key	✓	CipherTrust Manager protects and stores versioned backups and archives of keys. Backups are generated on the appliance and are stored there until deleted. They can be downloaded from the appliance and uploaded back to the same or to another appliance. When a backup is created, it is always encrypted with a backup key. If a backup key is not specified, the default backup key is used to encrypt the backup. This backup key is required to restore the backup file.
9.5.2	Key Recovery	✓	
9.5.3	System Redundancy/Contingency Planning	✓	CipherTrust Manager appliances in a clustered configuration with real-time replication of keys, policies, and configuration information across multiple appliances - enabling complete disaster recovery and business continuity. For large distributed enterprises that use multiple encryption solutions, keys can be centrally managed without making any perceptible impact on system performance.
9.5.3.1	General Principles	✓	Active/Active clustering for the high availability can be configured. This provides high assurance deployments ensuring 24x7 uptime to support key management and data encryption requirements. There are versioned backups and archives of keys. With key versioning management, CipherTrust Live Data Transformation ensures efficient backup and archive recovery to enable more immediate access. In a data recovery operation, archived encryption keys, recovered from the CipherTrust Manager, are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys. In the event that a key has been compromised Live Data Transformation can seamlessly rotate to a new key for data protection.
9.5.3.2	Cryptography and Key-Management-Specific Recovery Issues	✓	
9.5.4	Compromise Recovery	✓	

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com