White Paper

THALES

NIST 800-57 Recommendations for Key Management Requirements Analysis

thalestct.com

THALES

CYBERSECURITY

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.* [1]

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 responsible for multiple key management systems, resulting in inconsistent policies, different levels of protection, and escalating costs.

The simplest path through this maze is to transition to a centralized key management model which involves administering the full lifecycle of cryptographic keys and protecting them from loss or misuse. Transitioning to such centralized solution provides the ability to provide comprehensive key lifecycle management and auditability.

CipherTrust Data Security Platform

The CipherTrust Data Security Platform, developed by Thales, is an integrated, unified solution designed to address the full lifecycle of enterprise data security. It enables organizations to discover, protect, and control their most sensitive data—whether it resides on-premises, in the cloud, or across hybrid environments. With growing regulatory pressures and complex threat landscapes, CipherTrust provides a centralized architecture that simplifies compliance, reduces risk, and enforces consistent data protection policies across all environments. The platform supports a wide range of use cases, including data discovery, classification, encryption, access control, and activity monitoring, helping businesses maintain security and compliance without compromising operational agility.

Discovering Data

Understanding where sensitive data resides is the first step in any effective data protection strategy. The CipherTrust Platform offers robust discovery capabilities through CipherTrust Data Discovery and Classification (DDC). This tool automatically scans and classifies structured and unstructured data across file servers, databases, big data environments, and cloud storage. With built-in templates for regulatory compliance (such as GDPR, HIPAA, and PCI DSS), organizations gain visibility into sensitive data locations and types, allowing them to prioritize protection and remediate data exposure risks more efficiently.

Key Product: CipherTrust Data Discovery and Classification (DDC)

Controlling Data

Effective data security begins with control—ensuring that only authorized users, applications, and systems can access sensitive data, no matter where it resides. The CipherTrust Data Security Platform delivers centralized, policy-based access control that spans hybrid and multi-cloud environments, helping organizations reduce risk, enforce compliance, and maintain operational agility.

CipherTrust Manager (CM) serves as the central control point, enabling unified key lifecycle management, policy enforcement, and access auditing across the full data security ecosystem. It ensures consistent application of access control rules across databases, applications, file systems, and cloud platforms.

For organizations leveraging cloud-native services, CipherTrust Cloud Key Manager (CCKM) provides cloud key lifecycle management for Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) use cases across major cloud providers such as AWS, Microsoft Azure, Google Cloud, Salesforce, and more. It gives enterprises full visibility and control over cloud-native encryption keys, reducing risk and strengthening data sovereignty.

Enterprise Key Management (EKM) extends secure key lifecycle controls to internal and third-party systems, including databases and storage solutions, ensuring that cryptographic operations are governed by enterprise-defined policies. This allows organizations to consolidate key management under a single authority, minimizing complexity and improving audit readiness.

To support interoperability and integration across diverse environments, CipherTrust Key Management Interoperability Protocol (KMIP) provides standards-based connectivity to a wide array of encryption-enabled systems and third-party HSMs, enabling centralized control without sacrificing flexibility.

Finally, CipherTrust Cloud Application Key Management (CAKM) equips developers and DevOps teams with APIs to directly integrate key generation, storage, and use into cloud-native applications. This enables programmatic key access while ensuring that policies around key usage, separation of duties, and role-based controls are consistently enforced.

Together, these CipherTrust solutions enable organizations to implement fine-grained, auditable access controls across their IT landscape, from legacy infrastructure to cutting-edge cloud-native applications—ensuring that sensitive data remains secure, compliant, and under enterprise control at all times.

Key Products: CipherTrust Manager (CM), CipherTrust Cloud Key Manager (CCKM), CipherTrust Key Management Interoperability Protocol (KMIP), Enterprise Key Management (EKM), Cloud Application Key Management (CAKM).

Protecting Data

Protecting sensitive data—whether at rest, in use, or in motion—is the central mission of the CipherTrust Data Security Platform. Through a modular, extensible architecture, CipherTrust delivers a broad set of capabilities to secure unstructured files, structured databases, and transactional data across on-premises, cloud, and containerized environments.

CipherTrust Transparent Encryption (CTE) delivers robust, file-level encryption without requiring application changes, making it ideal for securing data in traditional and modern infrastructures alike. For organizations dealing with large-scale structured data transformations, CipherTrust Batch Data Transformation enables efficient rekeying and format-preserving encryption operations across massive data sets. When granular control over database protection is required, CipherTrust Database Protection offers column-level encryption to protect sensitive fields—such as PII or financial data—within leading relational databases.

For application-layer security, CipherTrust Application Data Protection enables direct integration with enterprise applications to secure sensitive data elements during creation or modification, while CipherTrust RESTful Data Protection allows developers to easily embed tokenization, encryption, and data masking into web applications via secure APIs. Additionally, CipherTrust Data Protection Gateway delivers runtime data protection for cloud-based applications, applying real-time, policy-based encryption and tokenization to sensitive fields as they enter or leave the cloud environment.

By combining these tools, organizations can enforce a consistent data protection strategy across diverse workloads, maintain regulatory compliance, and minimize the risk of data breaches without disrupting operations.

Key Products: CipherTrust Transparent Encryption (CTE), CipherTrust Application Data Protection (CADP), CipherTrust RESTful Data Protection (CRDP), CipherTrust Data Protection Gateway (DPG), CipherTrust Batch Data Transformation (BDT), CipherTrust Database Protection (CDP)

Monitoring Data

Effective data security doesn't end with protection — it requires continuous monitoring to detect misuse, assess exposure, and support compliance efforts. The CipherTrust Platform provides deep visibility into data activity through advanced monitoring capabilities such as Data Activity Monitoring (DAM) and File Activity Monitoring (FAM). These tools capture detailed logs of user and process interactions with sensitive data, enabling organizations to detect unauthorized access attempts, investigate anomalies, and meet audit requirements.

Building on this foundation, Data Risk Intelligence (DRI) analyzes discovered sensitive data and maps it against known risk indicators to identify where exposure is greatest. This enables security teams to prioritize high-risk data sets for remediation. Complementing DRI is Data Risk Analytics (DRA), which applies analytics and contextual insights — such as user behavior patterns, access frequency, and location — to evaluate the risk level associated with specific data interactions. These insights empower organizations to make informed decisions about access policies and risk response, enabling more adaptive and intelligent data security strategies.

Key Products: CipherTrust Data Activity Monitoring (DAM), CipherTrust File Activity Monitoring (FAM), CipherTrust Data Risk Intelligence (DRI), CipherTrust Data Risk Analytics (DRA)

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 CipherTrust Platform.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
6	**Protection Requirements for Key Information**		
6.1	Protection and Assurance Requirements	√	Thales provides key management solutions via CipherTrust Manager • physical appliances for deployment in data centers • virtual appliances for deplomet in public and private cloud CDSPaaS Key Management Service • SaaS offering hosted by Thales in Europe and the Americas These offerings fulfill the necessary requirements involving key generation and key lifecycle management. All Thales key management offerings can be configured to integrate with a FIPS 140 L3 certified Hardware Security Module (HSM) as a Root of Trust and source of key entropy.
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	√	All of the Thales key management offerings are deployed as hardened appliances and services. The key management software is compiled with the underlying operating system embedded to minimize attack vectors. In addition, appropriate access controls are embedded to ensure the management of the platform and usage of the keys generated are controlled. The appliance supports full disk encryption and can be deployed in high-availability, Active/Active clustered configurations. Each offering can support replication of keys, policies, and configurations. This enables seamless disaster recovery and business continuity across multiple instances.
6.2.1	Protection Mechanisms for Key Information in **Transit**	√	All Key Management offerings support backup of key material can provide software solutions and APIs to utilize said keys for cryptographic operations.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
6.2.1.1	Availability	√	CipherTrust Manager ensures high availability through clustered deployment options and redundant communication paths between nodes. Every CDSPaaS tenant is configured to deploy with Primary/Disaster Recovery sites to ensure the services meets its 99.95% SLA.
6.2.1.2	Integrity	√	Supports secure transmission of key materials and policies using TLS/SSL to maintain integrity during transit.
6.2.1.3	Confidentiality	√	Utilizes TLS-encrypted communications and optional client authentication to ensure confidentiality of key exchanges and administrative sessions.
6.2.1.4	Association with Usage or Application	√	All CipherTrust Key Management offerings support API (KMIP and REST) programmatic access to its keys as well as a browser based Management Console Additionally, Thales provdes CipherTrust Application Data Protection (SDKs for popular programming languages JCE, .NETCore and C) to simplify integration to specific usage contexts and applications.
6.2.1.5	Association with Other Entities	√	Keys can be explicitly associated with users, applications, or services through role-based and attribute-based access controls.
6.2.1.6	Association with Other Related Key Information	√	Offers granular access control via Roles or Attribute-Based Access Control (RBAC/ABAC), ensuring that keys are only used in authorized contexts The key management solutions also support • Secure key distribution using SSL/TLS • Protection of key hierachy by encapsulating all Data Encryption Keys (DEK) with a Master Encryption Key (MEK) residing in a Thales or 2rd party HSM.
6.2.2	Protection Mechanisms for Key Information in **Storage**	√	Access to keys can be controlled thru Access Controls mentioned previously. Customers can choose to only access keys from the key management platform or secuely cache the key for better performance (e.g. protection of credit card information during peak retail shopping periods).
6.2.2.1	Availability	√	Key policies are used to determine permissions to keys (either as part of an administrative function or access to the key to utilize it for encrypt or decrypt operations.)

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
6.2.2.2	Integrity	√	All key management solutions ship with a FIPS 140 cryptographic module in addition to the HSM integration mentioned previously. This signifies CipherTrust offers NIST Approved algorithms and functions in its solution.
6.2.2.3	Confidentiality	√	Thales offerings support the use of approved algorithms in a FIPS 140 L1-validated cryptographic module, using approved techniques that provides protection at the security strength that meets or exceeds the security strength required for the secret key information. AND The application of controls to protect the key (whether it be role or policy based) AND Physical, Virtual or SaaS offerings which provide controlled access to the key management product or service.
6.2.2.4	Association with Usage or Application	√	CipherTrust Manager binds keys to specific applications or data sets through policy-driven associations and APIs, ensuring precise usage control.
6.2.2.5	Association with Other Entities	√	Keys are mapped to users, roles, or services through defined policies and fine-grained access controls.
6.2.2.6	Association with Other Related Key Information	√	Relationships between keys and associated metadata (e.g., rotation dates, ownership, tags) are preserved and managed via policy

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
6.2.3	Metadata for Keys	√	Keys managed by CipherTrust Manager contain a single metadata record, which can link to multiple versions of the key. Each version is uniquely tracked, providing a detailed audit trail for compliance and lifecycle management.
7	**Key States and Transitions**		
7.1	Pre-activation State	√	CipherTrust Manager provides centralized key lifecycle management for all CipherTrust Data Security Platform products and services. Built on an extensible microservices architecture, it supports all standard key states—from generation through retirement—ensuring secure and auditable transitions throughout the lifecycle. Key management capabilities include: • State transitions such as activation, suspension, deactivation, compromise, and destruction • Role-based access control (RBAC) for fine-grained key and policy management • Multi-tenancy support to isolate keys and operations across users or departments • Comprehensive auditing and reporting for key usage, operational changes, and policy enforcement CipherTrust Manager also supports secure key generation, backup and recovery, and policy-driven actions. Additionally, the CipherTrust Data Security Platform as a Service Key Management Service (CDSPaaS KMS) extends these capabilities by offering a hosted solution for the key management service, removing the burden of system upgrades and maintenance.
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 supports comprehensive key management functions that are logically separated from standard operations. These functions include domain creation, key creation, host registration, system initialization, and audit logging. Thales also provides the ability to license non-production environments, enabling organizations to develop, test, and validate their data protection strategies before deploying to production.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
8.1.1	Entity Registration Function	√	The CipherTrust Data Security Platform supports robust entity registration by allowing secure onboarding of users, hosts, and applications. Each entity is authenticated and assigned appropriate credentials and access permissions, ensuring secure interactions with cryptographic services. System initialization is supported through policy-driven setup of cryptographic modules, key stores, and access controls. Administrators can configure trusted certificate authorities, security parameters, and network settings required to enable secure key management operations. During initialization, CipherTrust enables the creation and initialization of cryptographic domains and key hierarchies. This includes defining encryption policies, key attributes, and lifecycle parameters to ensure keys are created and managed in compliance with organizational and regulatory requirements.
8.1.2	System Initialization Function	√	
8.1.3	Initialization Function	√	
8.1.4	Keying-Material Installation Function	√	Encrypted communications between the CipherTrust key management appliance or service and agents are configurable. The platform supports TLS 1.2+ using its REST API to ensure secure key delivery and API access. Key establishment is created thru the configuration of the CipherTrust Connector portfolio (a series of software add-ons to support various key management and data encryption use cases).
8.1.5	Key Establishment Function	√	
8.1.5.1	Generation and Distribution of Asymmetric Key Pairs	√	CipherTrust supports the secure generation and deployment of encryption keys. The distribution of the keys from key management appliance or service is scenario dependent based on many factors, ranging from the application requirements to compliance guidelines which the customer is obligated to support. CipherTrust supports the creation of symmetric and asymmetric keys, as well as hashing . In addition, it uses certificates and can act as a Local or External Certificate Authority.
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	√	
8.1.5.1.3	Distribution of Centrally Generated Key Pairs	√	

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
8.1.5.2	Generation and Distribution of Symmetric Keys	√	Key generation supports standards-compliant symmetric algorithms and configurable key lengths Key distribution is supported via: Manual distribution (for controlled environments) Automated distribution and key wrapping Keys are associated with policies that define lifecycle states, access controls, and allowed usage
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	√	
8.1.5.2.2.3	Key Agreement	√	Support for key agreement protocols can be configured via CipherTrust Manager's API and agent-based workflows, depending on the environment and policy enforcement needs.
8.1.5.3	Generation and Distribution of Other Keying Material	√	CipherTrust Manager supports the secure generation and distribution of other cryptographic materials, such as initialization vectors, shared secrets, RBG seeds, asymmetric keys, random numbers, and passwords. These are passed between the CipherTrust Manager and hosts via a one-time-use AES-256 random key generated by the Manager. CipherTrust also offers Secrets Management via its partnership with Akeyless. Secrets Management is a cloud-native, SaaS platform that provides unified, vaultless management for all digital credentials (secrets like keys, passwords, certificates) across multi-cloud and hybrid environments, using patented Distributed Fragments Cryptography (DFC) for Zero-Knowledge security, eliminating single points of failure, and offering automated lifecycle management for DevOps.
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 Functionality	√	CipherTrust Manager supports automated key registration and lifecycle management, allowing keys to be registered during generation or securely imported from external systems. Registered keys are tagged, versioned, and governed by policies such as expiration, usage, and rotation.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
8.2	Operational Phase	√	CipherTrust Manager provides comprehensive tools for managing cryptographic keys throughout their operational lifecycle. This includes: • Key generation, import, export, and rotation • Support for symmetric and asymmetric key types • Control over key size, usage constraints, and policy enforcement All keys are stored in a centralized, hardware or virtual appliance, simplifying operations while enforcing strong access controls and auditability. CipherTrust Manager also supports Active/Active clustering for high availability, ensuring continuous uptime for encryption and key management services. All key usage is logged and can be exported to a variety of SIEM tools for reporting purposes
8.2.1	Normal Operational Storage Function	√	
8.2.1.1	Cryptographic Module Storage	√	CipherTrust supplies a secure key vault backed by a FIPS 140 L1, crypto module cryptographic module, ensuring isolation, protection, and compliance with international standards.
8.2.1.2	Immediately Accessible Storage Media	√	Keys are readily available to authorized services and applications during runtime, while access is tightly controlled through policy-based authorization, role-based access control (RBAC), and secure API communication.
8.2.2	Continuity of Operations Function	√	CipherTrust Manager supports high-availability deployments, including Active/Active configurations, for continuous access to keys and services. This architecture allows for automatic failover and synchronized replication, ensuring that encryption and key management operations continue uninterrupted even during system events or outages.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
8.2.2.1	Backup Storage	√	CipherTrust Manager uses backup encryption keys to securely protect key backups. Administrators can: • Generate a new backup encryption key, or • Reuse an existing key when creating backups Backup keys are stored encrypted using a secure vault within CipherTrust Manager. Each backup may include critical data such as user keys or database dumps, all encrypted according to the system's configured key hierarchy. A final encrypted backup file is generated using the designated backup key, ensuring secure recovery and compliance with retention and protection policies. CDSPaaS auto generates the backup of tenant key and configuration information and replicates this information to the DR location to support operational failover.
8.2.2.2	Key Recovery Function	√	CipherTrust Manager supports robust key recovery capabilities, including key, restore. Keys are versioned and archived, supporting rapid recovery when needed. During recovery, keys retrieved from backup are securely applied to the relevant datasets, with encryption maintained using current cryptographic policies.
8.2.3	Key Change Function	√	CipherTrust supports: • Key change for replacing compromised or outdated keys • Re-keying, enabling seamless replacement of keys without interrupting operations • Key update workflows that apply newer keys to older datasets as part of a versioned lifecycle process • All updates are governed by policy-based controls and audit logging for traceability.
8.2.3.1	Re-keying	√	
8.2.3.2	Key Update Function	√	

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
8.2.4	Key Derivation Methods	√	CipherTrust supports secure key derivation methods consistent with industry standards. Derived keys are created based on unique, application-specific inputs and comply with approved cryptographic standards for secure usage.
8.3	Post-Operational Phase	√	CipherTrust retains cryptographic materials per policy after their active use has ended, allowing for secure archival, auditing, or decommissioning.
8.3.1	Key Archive and Key Recovery Functions	√	CipherTrust supports secure archiving of retired or inactive keys. Archived keys remain accessible for approved recovery scenarios and are stored using encryption consistent with active key policies. Archived keys can be restored based on versioned metadata. Policy controls govern access and retention.
8.3.2	Entity De-registration Function	√	CipherTrust supports the use of Connectors for various key management and data encryption use cases. Administratrors can: • Register and manage client entities • View, modify, revoke, or delete client registrations as needed Once a client is deregistered, all communication between CipherTrust and the Connector endpoint is terminated, ensuring immediate and complete disassociation.
8.3.3	Key De-registration Function	√	Within CipherTrust Manager, a designated Key Admins group manages key de-registration. Admins have permissions to: • Create and manage their own keys • Perform operations on other keys based on their assigned privileges Key de-registration removes keys from operational use but retains metadata for audit if required.
8.3.4	Key Destruction Function	√	Only users in the System Defined Group have permission to permanently destroy keys (such as CTE policies and associated keys). • Keys marked for deletion are securely removed based on policy and usage state • Only unused or expired keys can be deleted, ensuring cryptographic continuity

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
8.3.5	Key Revocation Function	√	CipherTrust supports key revocation based on usage status or compromise events. Revoked keys are: • Immediately marked as inactive • Prevented from being used in future encryption or decryption operations • Tracked in audit logs for compliance and incident response
8.4	Destroyed Phase	√	The Destroyed Phase ensures that cryptographic keys are irretrievably deleted when no longer needed. • Only authorized administrators (e.g., CTE Admins) can initiate destruction • Keys must be inactive or non-operational before destruction • Destruction operations are logged to maintain audit integrity
9	**Additional Considerations**		
9.1	Access Control and Identity Authentication	√	CipherTrust enhances access control through kernel-level agents and AES-256 encryption, surpassing typical OS-level controls. It enforces least privilege access, allowing only authenticated administrators and clients to communicate with the key manager. Integration with role-based access controls ensures secure, policy-driven identity management.
9.2	Inventory Management	√	CipherTrust provides centralized inventory visibility and lifecycle management for all cryptographic keys and certificates across the CipherTrust Data Security Platform. Its microservices-based architecture simplifies operations such as key generation, rotation, backup, archival, and deletion.
9.2.1	Key Inventories	√	All cryptographic keys are cataloged with metadata such as key type, usage, status, creation date, and expiration, enabling full visibility and control across environments.
9.2.2	Certificate Inventories	√	CipherTrust tracks certificates used for encryption, authentication, and digital signing. Each certificate is indexed for quick retrieval and lifecycle management.
9.3	Accountability	√	All user and administrative actions within CipherTrust are fully auditable and attributable through detailed logs. These logs include timestamps, user roles, affected objects (e.g., keys, policies), and the nature of each action, helping ensure accountability and support for internal or external audits.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
9.4	Audit	√	CipherTrust generates comprehensive audit logs capturing all key lifecycle operations (e.g., generation, access, modification, rotation, deletion). Logs are tamper-resistant and can be forwarded to external SIEM systems or retained locally for compliance. This capability ensures full traceability for audit and compliance purposes.
9.5	Key-Management System Survivability	√	CipherTrust supports high availability through clustered deployments with real-time replication of keys, policies, and configuration data across appliances. This architecture supports: • Seamless failover and disaster recovery • No disruption to cryptographic operations • Centralized key management across distributed environments with minimal performance impact
9.5.1	Backed Up and Archived Key	√	CipherTrust automatically creates versioned backups of all cryptographic keys. Backups: • Are stored securely on the appliance • Remain available until explicitly deleted • Can be restored on the same or another appliance • Are always encrypted using a designated backup key If a specific backup key is not provided, a default backup key is used to ensure data protection and future recovery.
9.5.2	Key Recovery	√	During key recovery, backup files—encrypted using the assigned or default backup key—can be: • Downloaded from the appliance • Re-uploaded to the same or a different CipherTrust appliance • Decrypted and restored using the required backup key This enables secure restoration of archived encryption keys for operational continuity and compliance with retention policies. For CDSPaaS, backups are controlled by the DevOps team and can be restored to point in time for recovery.

NIST 800-57 Reference	Requirement	Requirement Met	CipherTrust Platform
9.5.3	System Redundancy/Contingency Planning	√	CipherTrust supports robust system redundancy and contingency planning through clustered deployments with real-time replication of keys, policies, and configurations across multiple appliances. • This setup ensures high availability, seamless failover, and disaster recovery • Organizations with multiple encryption endpoints can centrally manage keys without disrupting system performance • Business continuity is preserved even during infrastructure failure scenarios
9.5.3.1	General Principles	√	CipherTrust supports Active/Active high availability deployments to ensure minimal downtime. • Designed for 24x7 operations with full support for uninterrupted key management and encryption services • All keys and related policies are versioned and securely stored, allowing seamless recovery in the event of failure or compromise
9.5.3.2	Cryptography and Key-Management-Specific Recovery Issues	√	CipherTrust maintains comprehensive backups and versioning of keys. These capabilities allow: • Recovery of archived encryption keys aligned with the original version of protected data • Secure application of keys to historical datasets through Live Data Transformation, preserving data integrity • Controlled and auditable recovery procedures in line with cryptographic best practices
9.5.4	Compromise Recovery	√	In the event of a key compromise, CipherTrust enables recovery via Live Data Transformation, which allows data encrypted with a compromised key to be seamlessly re-encrypted using a new, secure key. • This eliminates the need to re-ingest or decrypt raw data manually • Recovery operations are automated, secure, and aligned with enterprise-grade data protection policies

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

THALES

Contact us

For office locations and contact information,
please visit thalestct.com/contactus

thalestct.com