White Paper

Thales
Key Management

Simplify data security by centrally managing keys and policies across the enterprise

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

THALES
Building a future we can all trust

Executive Summary

Today, every IT organization is striving to protect valuable digital assets from accidental exposure or intentional misuse. To meet various digital privacy regulations and compliance mandates, many organizations have deployed a variety of point encryption solutions as a primary method of protecting sensitive data. Unfortunately, the majority of disparate encryption solutions have fallen short in addressing enterprise key management challenges and the result is a weakened security posture, increases in failed audits and more security breaches.

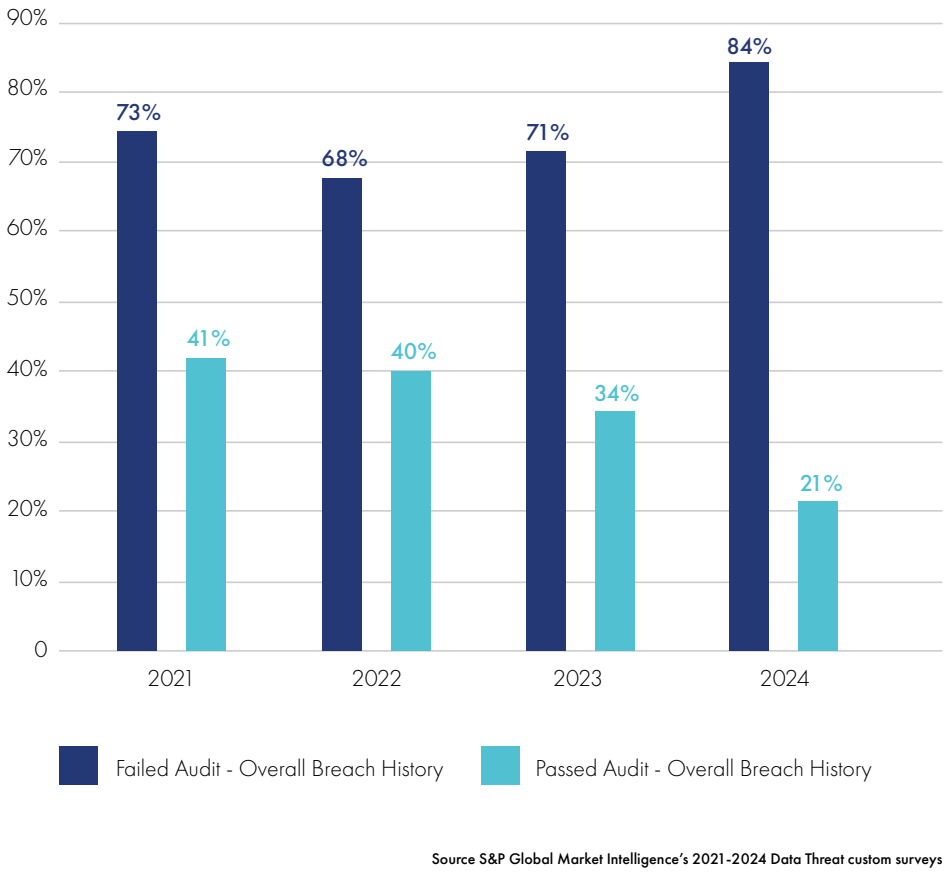
This white paper looks at the evolution of encryption and key management systems, and examines the major challenges faced by IT teams for encryption systems, including regulation and compliance, complexity, and management tools. The review of major challenges is followed by a review of recent industry initiatives and compliance regulations that are shaping the future of key management.

The paper concludes with an introduction to CipherTrust Manager, the next-gen enterprise key management offering from Thales. CipherTrust Manager provides a powerful integrated solution that enables organizations to centrally manage encryption keys and policies for CipherTrust Connectors and third-party KMIP-compliant products.

Data Security Challenges

To drive operational efficiency into their data-intensive processes, many organizations are adopting digital transformation and migrating their applications and data to the cloud. Data migration to third-party hosted environments and multiple cloud service providers is creating new attack surfaces that cybercriminals can exploit, as a result, data breaches threaten the IT landscape at an increasing rate. All of this adds up to today's data environments becoming even more complex – which is a top barrier to data security.

In the 2024 Thales Data Threat Report (which is based on an S&P Global survey of nearly 3,000 respondents across 18 countries who have responsibility or influence over IT and data security), operational complexity remained a security concern and human error was reported to be the leading cause of data breaches (31%). It wasn't surprising to see a strong correlation between achieving compliance and reducing breaches.



Source S&P Global Market Intelligence's 2021-2024 Data Threat custom surveys

Figure 1: Correlation between passing audits and experiencing fewer security breaches

Ransomware attacks are more common, with 28% of respondents experiencing an attack in 2023, up from 22% in 2022. Multi-cloud continues to be a reality regardless of cloud maturity but in 2024 enterprises can better abstract their controls so that they are more applicable to multiple jurisdictions and changing market requirements.

Looking Back at Encryption and Key Management Techniques

The Internet has been the most significant driving force in the evolution of encryption and key management technologies. Providing easy access to a company's data for authorized users (employees, partners and customers) has taken priority, with data security being implemented as an afterthought. Connecting public and private resources to any company's sensitive data increases the risk of data breaches.

In response to the increasing threat volume, complexity and severity, a variety of perimeter, endpoint security controls and security policies have been adopted and data privacy regulations and compliance requirements have been developed. Potentially exploitable gaps between the controls and policies can be mitigated with simplified encryption and key management. This white paper explains the importance of resolving the difficulties of disparate native key repositories scattered across various information systems in the enterprise.

Data Encryption Across Disparate Systems → Security Silos

The increased adoption of encryption solutions has improved security for enterprises, but managing a variety of cryptographic keys has made life much more challenging for the IT and security teams. Nearly all offline data storage devices and many database management systems (DBMS) include the option of embedded native encryption capability. The islands of encryption from disparate providers results in keys and key management software that frequently don't interoperate well with one another.

System administrators and database administrators (DBAs) end up becoming the managers of encryption keys specific to data storage, database management systems and applications. The security silos distract from the primary tasks of IT and database administration, putting an enterprise's overall security posture at risk.

The Business Problem - Siloed Data

Without a centralized encryption key management solution, security administrators are faced with a costly, inefficient and often impossible task — managing disparate encryption keys for many different data storage, database management systems and applications accumulated over time from separate vendors. A heterogeneous environment means that an enterprise using native TDE to secure databases, such as Oracle and Microsoft SQL Server, has to factor in the increased risk and administrative resources required to manage multiple incompatible encryption solutions. Managing a separate encryption system for each data store is costly, complex and error-prone due to inconsistent security policies and processes, as shown in Figure 2 below.

When each system administrator controls encryption keys separately for each data repository they manage, the keys are generally stored in the same location as the encrypted data, creating an opportunity for security compromise – the electronic equivalent of taping the key onto the front door.

Using manual systems to store and transmit encryption keys, weak password control, or failing to revoke keys when an employee leaves the organization, makes strict adherence to compliance requirements nearly impossible and data breaches are likely to occur.

Figure 2: Costly and complex to manage data silos

Essentials of Enterprise Key Management

As organizations deploy an ever-increasing number of encryption solutions, they can decrease the risk of a breach or non-compliance by using a centralized key management solution that enables them to securely store and backup/restore the encryption keys, define consistent access control policies, audit all key management operations and separate encryption tasks from key management tasks.

Here are the essential elements of a robust enterprise key management solution that can help address data security challenges.

Secure Key Storage

Secure key storage is the foundation for any enterprise key management system. The use of Hardware Security Modules (HSMs) is a well-established approach for protecting encryption keys. Mandated in government and certain financial/payment markets, HSMs protect cryptographic keys and perform various cryptographic functions in a secure tamper-resistant environment. Enterprise key management solutions should provide options to support built-in HSMs, external network-attached HSMs or a cloud-based HSM-as-a-service, based on the level of assurance your company needs – whether it is FIPS 140 L1 or L3.

Centralized Key Lifecycle Management

The key management system (KMS) should be able to centrally manage keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation and deletion. The KMS should also provide policy-based access control to keys, support various authentication providers including Active Directory and LDAP, and robust auditing of all key management operations.

Enabling Scalability and Flexibility

As the complexity of an organization's IT infrastructure grows from a single onsite datacenter to external hosted environments to multiple cloud service providers, the enterprise key management solution should be flexible enough to adapt to changing requirements for sensitive data.

A flexible key management solution supports on-premises infrastructure and is deployable as a virtual appliance in public cloud environments such as AWS, Azure, Google Cloud, Oracle, Salesforce and SAP, private clouds such as VMware vSphere, Microsoft Hyper-V and Nutanix AHV, and hybrid clouds such as Azure Stack.

Interoperability with Third-party Systems

Recommended enterprise key management solutions support the following three major interoperability standards that enable you to work with multiple server, storage and device vendors who use the keys for authentication, digital signing or encrypting data.

- PKCS#11 – Public Key Cryptographic Standard #11 (PKCS#11) specifies an API for devices to interoperate with hardware security modules (HSMs) and smart cards that hold cryptographic tokens. PKCS#11 is also used to access signing keys from Certification Authorities (CAs) or to enroll user certificates for digital signing and encryption using asymmetric keys. As an example, Oracle TDE uses PKCS#11.
- EKM/MSCAPI – Extensible Key Management (EKM) using the Microsoft Cryptographic APIs (MSCAPI), enables MS SQL Server to communicate with third-party key management servers. The keys must be exported from a provider before they are stored in the database. This approach enables key management that includes an encryption key hierarchy and key backup for Microsoft SQL Server Transparent Data Encryption.
- OASIS KMIP – Key Management Interoperability Protocol (KMIP), maintained by the Organization for Advancing Open Standards for the Information Society (OASIS), defines the standard protocol for any key management server to communicate with clients (e.g., storage devices, databases) that use the keys for embedded encryption. KMIP enables interoperability for key lifecycle management between encryption systems and enterprise applications.

Facilitate Governance and Reporting

The most important aspect of governance is a discipline for managing, controlling, and protecting the security and privacy of data. A policy-driven key management system forces the adherence to procedures for separation of duties and user authorization, and automates all the security processes involved in the key lifecycle. Some of the more notable industry standards and compliance requirements affecting key management today include:

- **Payment Card Industry Data Security Standard (PCI DSS)**
  Any organization that plays a role in processing credit and debit card payments must comply with the strict PCI DSS compliance requirements for the processing, storage and transmission of account data. PCI DSS tests span a wide variety of common security practices along with technologies such as encryption, key management, and other data protection techniques. The latest update to the standard, PCI DSS 4.0, in force since April 2024, includes a shift to a more risk-based and customized approach.
- **General Data Protection Regulations (GDPR)**
  Perhaps the most comprehensive data privacy standard to date, GDPR affects every organization that processes the personal data of EU citizens - regardless of where the organization is headquartered. GDPR is designed to improve personal data protections and increase organizational accountability for data breaches. With potential fines of up to four percent of global revenues or 20 million EUR (whichever is higher), the regulation impacts many businesses.
- **UIDAI's Aadhaar Number Regulation Compliance**
  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.
- **Gramm Leach Bliley Act (GLBA)**
  The United States requires that firms acknowledge publicly when a disclosure event occurs. Led by California's Database Security Breach Notification Act in 2003, more than half of all states have passed additional rules beyond the general notification requirements of GLBA to require firms to notify disclosure victims of the event, with higher associated costs to the business than GLBA exacted.
- **The U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act**
  HITECH does not require breach notification if the Protected Health Information (PHI) being exposed in the event of a data breach is already encrypted. For "unsecured PHI data", notification of the breach to every individual affected must be made. With the increasing cost of recovering from a data breach, it is important to invest in a strong encryption strategy for PII and PHI data, with centralized key management as its foundation.
- **Network and Information Security Directive 2 (NIS2)**
  The European Union's NIS2 is a legislative act that aims to achieve a high common level of cybersecurity for organizations across the European Union. NIS2 requires operators of critical infrastructure and essential services in the EU to implement appropriate security measures that include encryption, policies and procedures regarding the use of cryptography and access management.

- **Digital Operational Resilience Act (DORA)**
  The DORA Act harmonizes the operational resilience rules applying to 20 different types of financial entities. The new regulation requires financial entities, and their IT service providers, such as cloud platforms, to implement measures to improve the digital operational resilience of the sector, including the protection of data at rest, in use, and in motion, and the protection and management of cryptographic keys.

Introducing CipherTrust Manager

The Foundation of Thales Key Management Solutions

CipherTrust Manager enables organizations to meet their data privacy and compliance requirements by centrally managing encryption key lifecycles and policies, independent of where the data resides. CipherTrust Manager simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion. CipherTrust Manager provides role-based access control to keys and policies, multi-tenancy support with ultimate separation of duties, and robust auditing and reporting of all key management operations.

The unified management console in CipherTrust Manager makes it easy to discover and classify data, and protect sensitive data using a comprehensive set of data protection Connectors from Thales.

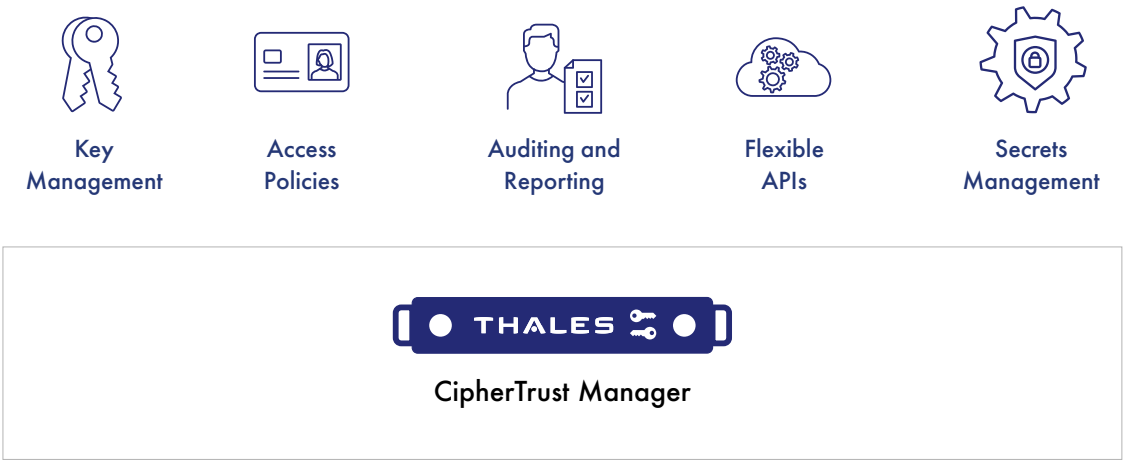


Figure 3: CipherTrust Manager

Key Benefits

Simplified Management

CipherTrust Manager provides a unified management console that enables you to discover and classify sensitive data, and protect data using integrated Thales Data Protection Connectors across on-premises data stores and multi-cloud deployments. It offers advanced self-service licensing for improved visibility and control of licenses.

Cloud-friendly Deployment

CipherTrust Manager offers users additional hosting options, and can run as a native virtual machine on AWS, Microsoft Azure, Google Cloud, VMware, Microsoft HyperV and more. Additionally, native support for CipherTrust Cloud Key Management is available on CipherTrust Manager to streamline key management across multiple cloud infrastructures and SaaS applications.

Flexible Form Factors

- CipherTrust Manager is available in both virtual and physical form factors. Flexible deployment options can easily scale to provide key management at remote facilities or in cloud infrastructures.
- CipherTrust Manager supports managing Key Encryption Keys (KEKs) in the FIPS 140 L3 boundary of Luna Network HSM.

Thales Enterprise Key Management Solutions

Thales Enterprise Key Management solutions are built on CipherTrust Manager. CipherTrust Manager serves as a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise, simplifying the administrative challenges around encryption key management, ensuring that keys are secure and always provisioned to authorized encryption services.

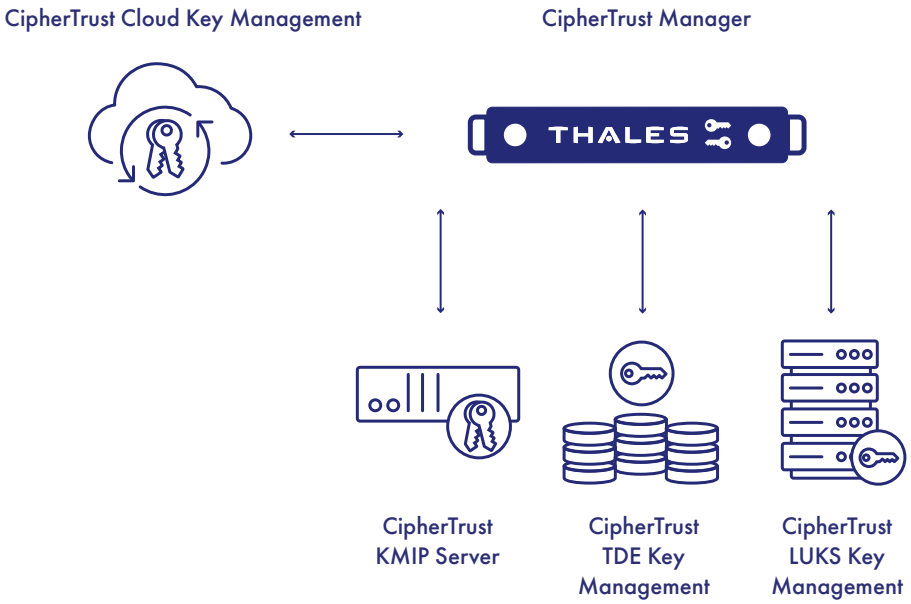


Figure 4: CipherTrust Cloud Key Management and CipherTrust Enterprise Key Management Solutions

CipherTrust Enterprise Key Management solutions enable organizations to centrally manage and store cryptographic keys and policies for the following third-party products as shown in Figure 4. The following three elements comprise the CipherTrust Enterprise Key Management solution.

- KMIP Server: Manages encryption keys across multiple KMIP clients (legacy data storage, cloud and virtual environments, SAN and NAS storage arrays, self-encrypting drives, and hyper-converged infrastructure solutions). Provides a simple interface to the key management functions on CipherTrust Manager, delivering powerful, centralized key management capabilities for KMIP-compliant applications/systems.
- TDE Key Management: Simplifies transparent data encryption (TDE) across Oracle TDE and Microsoft SQL Server TDE databases using TDE Key Agents, and keeps the TDE keys separate from your database servers.
- LUKS Key Management: Linux Unified Key Setup (LUKS) Key Management enables you to centrally manage encryption keys for Linux disk partitions. Provides transparent disk encryption.

CipherTrust Manager additionally integrates with a collection of powerful Connectors:

- CipherTrust Cloud Key Management (CCKM) manages keys for multi-cloud environments and services including AWS, Azure, GCP, Oracle, Salesforce and SAP
- CipherTrust Secrets Management (CSM) is an enterprise-grade secrets management solution which protects and automates access to secrets
- CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP) provides active behavior monitoring and data analytics, looking for abnormal I/O activity on a per-process basis
- CipherTrust Data Protection Gateway (DPG) offers transparent data protection to any RESTful web service or microservice leveraging REST APIs

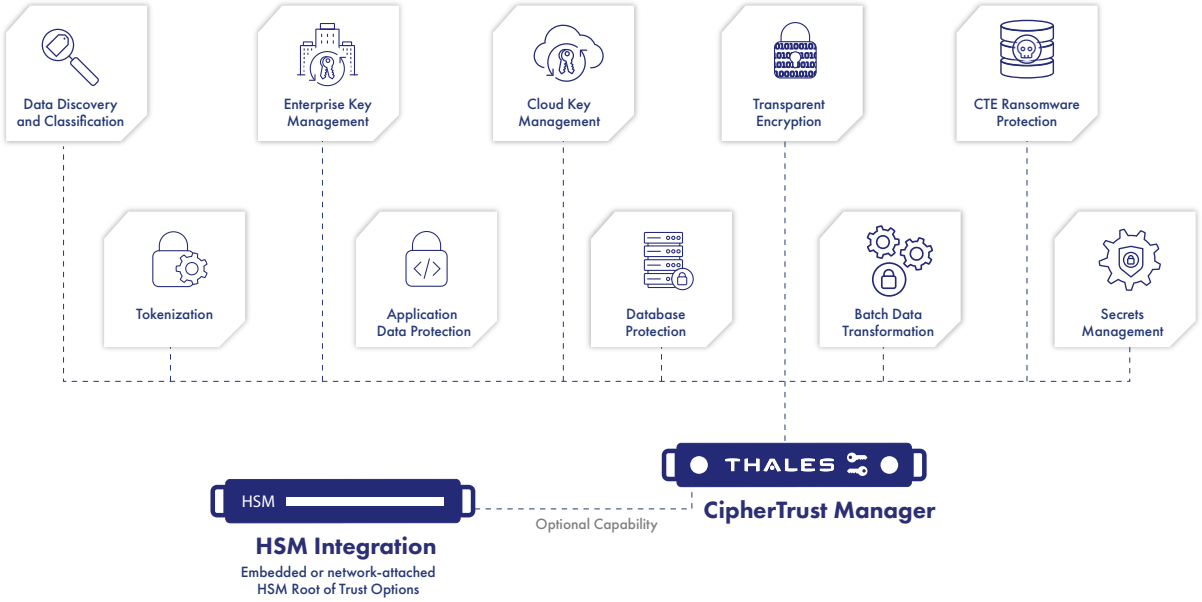


Figure 5: CipherTrust Manager and Thales Connectors comprise the Thales CipherTrust Data Security Platform.

Thales Hardware Security Module Solutions

Thales offers a variety of hardware security modules (HSMs), which are the highest performing, most secure and easiest HSMs to integrate in the market today. HSMs act as trust anchors to protect the master keys that encrypt your data and digital identities in a high assurance FIPS 140 Level 3-validated, tamper-resistant appliance. Thales offers the following types of purpose-built HSMs:

- General Purpose HSMs (Luna HSMs) come in several form-factors — a network-attached appliance, an embedded PCI module, and a portable USB appliance. Luna HSMs can easily be integrated with a wide range of applications to accelerate general cryptographic operations. The embedded PCI module is a Luna HSM PCI card available as an option in the CipherTrust Manager model k570.
- Cloud HSMs are available in the Data Protection On Demand (DPoD) online marketplace which provides a wide range of Cloud HSM and key management services.

Summary

Data is only as secure as the system that manages the encryption keys protecting the data. A centralized enterprise key management solution is critical to ensuring all sensitive enterprise data is secure and available. CipherTrust Manager helps organizations maximize IT efficiency through a centralized, extensible platform-based solution, and supports the burdens of encryption key management across the enterprise and into the cloud – without disrupting existing application or database environments.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

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