

Enterprise key management solutions



Challenges

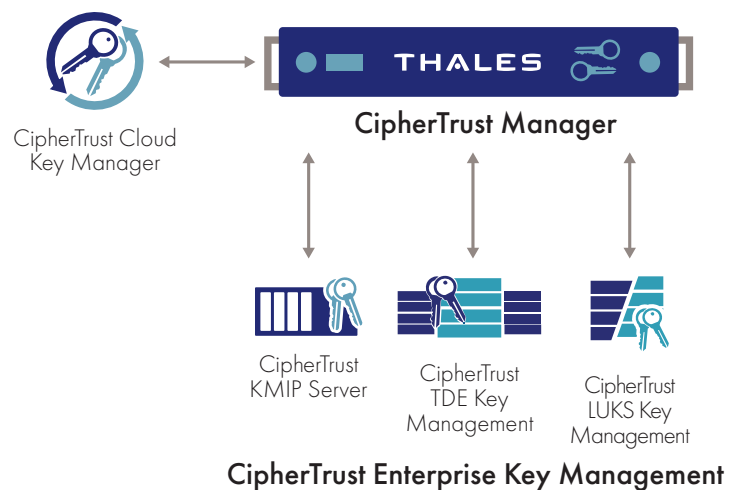
Managing encryption keys as a centralized service is essential to the integrity of any enterprise encryption system. Many organizations operate multiple, independent encryption systems resulting in silos, which complicates key management and erodes security. Managing keys for these silos consumes time, resources and budget. It also risks compromising data, if keys are kept local to the encryption systems they protect.

Solution: Thales key management solutions

Thales CipherTrust key management products centralize key management for internal as well as commercial off the shelf (COTS) applications. This gives customers greater command over your keys while increasing encryption data security. Thales CipherTrust key management products connect with your applications through standard interfaces and deliver access to robust key management and encryption functions.

Highly secure and efficient centralized key management

- Streamlined operations through centralized key management
- Improved compliance by separating keys from applications
- Comprehensive key services delivered by dedicated, FIPS-compliant hardware and software solutions



CipherTrust Manager: the foundation for Thales key management solutions

CipherTrust Manager is a high-availability appliance that centralizes encryption key management for the Thales Data Security Portfolio and third-party encryption solutions. CipherTrust Manager helps direct key life-cycle tasks including generation, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets.

CipherTrust Manager enhances key management by delivering strong separation of duties for increased security. Additionally, CipherTrust Manager offers multi-tenancy, or domains, allowing customers and service providers to generate unique key management environments. This provides additional security and ultimate separation of duties, where no single administrator has access to all domains.

CipherTrust Manager is available as either hardware or a virtual appliance. Either appliance is hardened to ensure protection of its contents and prevents any modification to the underlying operating system. In addition, non-HSM enabled appliances can utilize an external HSM as a root of trust for better security as well as utilize its random number generator for better key entropy.

Thales key management solutions

Thales key management solutions support a variety of applications, including:

Key Management Interoperability Protocol (KMIP)

KMIP is an industry-standard protocol for encryption key exchange between clients (appliances and applications) and a server (key store). Standardization facilitates external key management for storage solutions including SAN and NAS storage arrays, self-encrypting drives and hyper-converged infrastructure solutions. KMIP simplifies the requirement of separating keys from the data being encrypted, and allowing those keys to be managed with a common set of policies from a corporate perspective. CipherTrust Manager has already been certified with a number of 3rd party applications utilizing KMIP (as well as other API's).

Database and Linux Key Management

Thales centralized key management solutions for databases and Linux can provide high security while providing enhanced IT efficiency. For both Transparent Database Encryption (TDE) key management and Linux Unified Key Setup (LUKS), a Thales agent on the database or Linux server requests keys from CipherTrust Manager and serves them to TDE or LUKS.

Cloud Key Management using CipherTrust Cloud Key Manager

CipherTrust Cloud Key Manager delivers efficient, secure control over the full lifecycle of software as a service (SaaS) and infrastructure as a service (IaaS) encryption keys, including key creation, uploading, updating, storing, revocation and reporting. It is available as a service in the cloud and as an on-premises deployment using the CipherTrust Manager to securely manage keys.

CipherTrust Cloud Key Manager supported clouds include Microsoft Azure and Office 365, Amazon Web Services, Salesforce.com and IBM Cloud.



CipherTrust Key Management Solutions for Proprietary Applications

For the most convenient integrations into applications that perform encryption but require centralized, key management, the CipherTrust Manager offers PKCS# 11, REST, and NAE-XML API's that can be leveraged by any application environment supporting these API's. In addition, for the most performance-sensitive applications, CipherTrust Manager provides application-layer libraries implementing Java, C, C++, .NET and .NET CORE that can be installed on supported application server environments.

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.