cpl.thalesgroup.com

THALES

CipherTrust Data Security Platform

Discover, protect and control sensitive data anywhere with next-generation unified data protection

Discover Protect Control

Data Sheet

CipherTrust Data Security Platform

As security breaches continue to happen with alarming regularity and data protection compliance mandates get more stringent, your organization needs to extend data protection across more environments, systems, applications, processes and users. With the CipherTrust Data Security Platform from Thales, you can effectively discover, protect and control your organization's sensitive data anywhere with next-generation unified data protection.

The CipherTrust Data Security Platform integrates data discovery, classification, data protection and granular access controls, all with centralized key management. This solution removes data security complexity, accelerates time to compliance, and secures cloud migration, which results in fewer resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

The platform offers capabilities for discovering, protecting and controlling access to databases and files—and can secure assets residing in cloud, virtual, big data and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements, and it prepares your organization to nimbly respond when the next security challenge or compliance requirement arises.

Capabilities

- Centralized management console
- Monitoring and reporting
- Data discovery and classification
  - Risk analysis with data visualization
- Data protection techniques
  - Transparent encryption for files, databases and big data
  - Application-layer data protection
  - Format preserving encryption
  - Tokenization with dynamic data masking
  - Static data masking
  - Privileged user access controls
- Centralized enterprise key management
  - FIPS 140-2 compliant enterprise key management
  - Unparalleled partner ecosystem of KMIP integrations
  - Multi-cloud key management
  - Transparent Data Encryption (TDE) key management

Environments

- IaaS, PaaS and SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, IBM Cloud, Salesforce, Microsoft Office365, Service Now, Oracle Cloud, and more.
- Suported OSs: Linux, Windows and Unix
- Big data: Hadoop, NoSQL, SAP HANA and Teradata
- Database: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase and others
- Any storage environment

Platform advantages

- Discover, protect and control your organization's sensitive data anywhere with next-generation unified data protection
- Consistent security and compliance across physical, virtual, cloud and big data environments
- Flexibility and extensibility enable fast support of additional use cases
- Hardware Security Modules as the secure root of trust for the platform including FIPS 140-2 Level 3 certification

Key benefits

Simplify Data Security. Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform simplifies data security administration with a 'single pane of glass' centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud. Organizations can easily uncover and close privacy gaps, prioritize protection, and make informed decisions about privacy and security mandates before a digital transformation implementation.

Accelerate Time to Compliance. Regulators and auditors require organizations to have control of regulated and sensitive data along with the reports to prove it. CipherTrust Data Security Platform capabilities, such as data discovery and classification, encryption, access control, audit logs, tokenization, and key management support ubiquitous data security and privacy requirements. These controls can be quickly added to new deployments or in response to evolving compliance requirements. The centralized and extensible nature of the platform enables new controls to be added quickly through the addition of licenses and scripted deployment of the needed connectors in response to new data protection requirements.

Secure Cloud Migration. The CipherTrust Data Security Platform offers advanced encryption and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored.

Featured products:

CipherTrust Manager is the central management point for the platform, providing key and data access policy management. It is available in both physical and virtual form factors that are up to FIPS 140-2 Level 3 compliant.

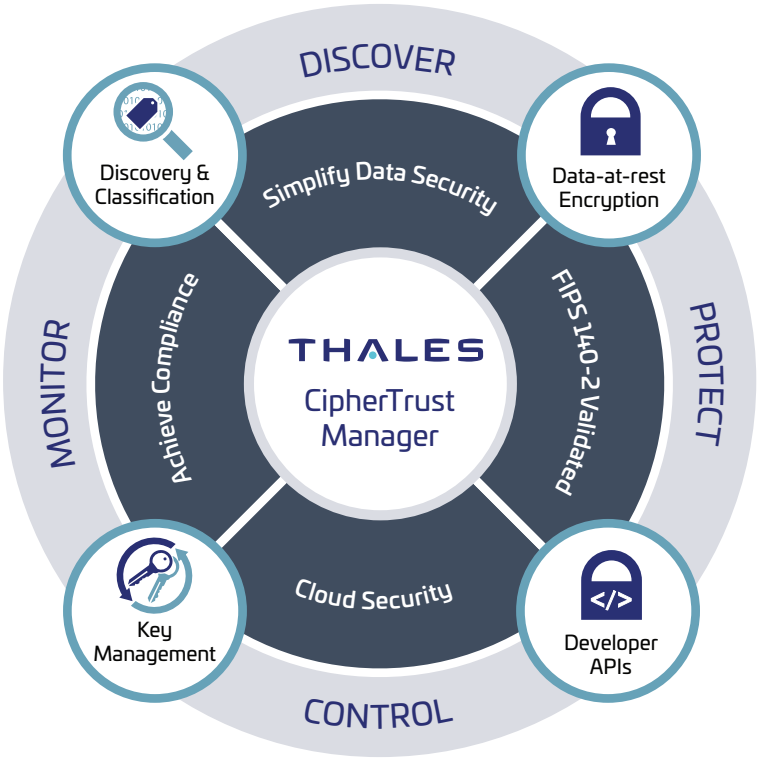
Data Discovery and Classification enables organizations to discover and classify sensitive data from a single pane of glass. Organizations can understand risks, uncover gaps, and make better decisions about both third-party data sharing and cloud migration.

CipherTrust Enterprise Key Management manages encryption keys for many sources and environments across the enterprise, simplifying encryption key management. The CipherTrust KMIP Server operates on CipherTrust Manager to centralize key management for many KMIP clients and partner verified solutions. CipherTrust Transparent Data Encryption (TDE) Key Management is available for many popular databases, and the CipherTrust Cloud Key Manager offers cloud Bring Your Own Key (BYOK) life cycle management for many Infrastructure-, Platform- and Software as a Service cloud providers.

Data-at-Rest Encryption protects data without requiring any changes to business or data management processes. CipherTrust Transparent Encryption encrypts data across on-premises, cloud, database and big data environments with comprehensive data access controls that can stop the most pernicious attacks. Extensions such as Live Data Transformation enable zero-downtime data encryption and key rotation.

The CipherTrust Data Security Platform offers a range of products with developer-friendly application programming interfaces for Key Management, Encryption and Tokenization. CipherTrust Application Data Protection provides server-or RESTful API-based key management and encryption services. CipherTrust Tokenization solutions include both Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization for customer choice based on use-case requirements.

CipherTrust Database Protection solutions provides database column-level encryption without the need for software engineering assistance. The solutions deliver the highest level of separation of duties for access to sensitive data.



CipherTrust Manager

Overview

At the center of the CipherTrust Data Security Platform is CipherTrust Manager, which centralizes keys, management and policies for all CipherTrust Data Security Platform products. Built on an extensible microservices architecture, CipherTrust Manager enables organizations to efficiently address privacy and data protection regulatory mandates and adapt readily as encryption and IT requirements evolve.

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 core features of the product.

CipherTrust Manager is available in both virtual and physical appliance form factors to address varying deployment use cases from public and private cloud to on-premises, secure deployment with physical security controls. For the highest level of root-of-trust quality, hardware appliances can leverage an embedded, FIPS 140-2 Level 3-compliant Luna PCI HSM. Hardware and virtual appliances can leverage Luna Network HSMs or one of several other network-attached HSMs.

Active/Active clustering for the highest availability can be configured with a mix of hardware and virtual appliances. This provides customers with high assurance deployments ensuring 24x7 uptime to support key management and data encryption requirements.

Benefits

- Centralized key management to allow consolidation of on-premises and cloud encryption keys across multiple applications, data stores, and appliances
- Provides the foundation for the Ciphertrust Data Security Platform, allowing customers the ability to reduce business risk with data discovery, classification and sensitive data protection
- Simplified management with a self-service licensing portal and visibility into licenses available and in use
- Cloud friendly deployment options with support for AWS, Azure, Google Cloud, VMware, Oracle Cloud, OpenStack and more
- Expanded Hardware Security Module (HSM) support for superior key control and generation
- Extensible microservices architecture enabling maintenance and upgrades without downtime
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and cloud vendors

Key features

- Full Key Lifecycle Management, including secure key generation, rotation, deactivation, deletion, and backup/restore
- Centralized administration, unifying key management operations with role-based access control and full audit log review.
- Self-service licensing, streamlining connector license provisioning and ongoing management
- Secrets management, providing the ability to create and manage secret and opaque objects for use on the platform
- Multi-tenancy provides capabilities required to create multiple domains with separation of duties to support large enterprise environments.
- REST APIs to automate repetitive management and encryption tasks
- Flexible HA clustering and intelligent key sharing, offering clustering physical and / or virtual appliances
- Robust auditing and reporting, including tracking key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) for easy integration with SIEM tools.

CipherTrust Manager Technical Specifications

Hardware Specifications (k470, k570)

Chassis Dimensions	19.0"(W) x 21"(D) x 1.75"(H)
Weight	12.7 kg(28lbs)
CPU	Intel Xeon E3-1275v5
Memory	16 GB
Hard Disk and Protections	1 X 2TB SATA SE (Spinning Disk)
Serial Port	1
Ethernet / NICs	4x1GB or 2x10GB/2X1GB
Power Supplies	• Average power (Watts) 0.7A @120V (84W) • Maximum power (Watts) 0.83A @120V (100W) • Voltage: 100-240V 50-60Hz
Power Cord Options	• PSE certified • Multiple country profiles
MTBF Telcordia	153,583
Chassis Intrusion Detection	Tamper seals. k570 Embedded HSM will zero itself upon tamper detection
Operating Temperature	0 to ~35°C
Non-Operating Temperature	-20 to 60 °C
Operating Relative Humidity	5% to 95% non-condensing
FIPS 140-2 Certifications	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3519
Embedded HSM Administration	k570 (Built in Thales Luna HSM), Management Console and REST API for HSM configuration
Mounting Hardware	• Non-sliding rail hardware and locking mounts included • Sliding rails available

Software Specifications

Administrative Interfaces	Web-based management console, REST API, ksctl (Command Line Interface), NAE XML			
Max Keys	k470 1M	k570 1M	k170v 25K	k470v 1M
API Support	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
Security Authentication	• Local User • AD/LDAP		• Certificate based authentication • k570: Local or Remote PED for master key setup and configuration	
Supported HSMs for Root of Trust	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, Data Protection on Demand, AWS CloudHSM			
Cluster Support	Active/Active. Max nodes=10 cluster Cluster members can be any model physical/virtual. k170v limited to 2-node clusters			
Backup	Manual and scheduled; option for HSM key to encrypt CM backup			
Network Management	SNMP v1, v2c, v3, NTP, Syslog-TCP			
Syslog Formats	RFC-5424, CEF, LEEF			
Software Certifications and Validations	k570 embedded Thales Luna HSM: FIPS 140-2 L3 for embedded Luna HSM			

Specifications for Virtual Machine Deployment

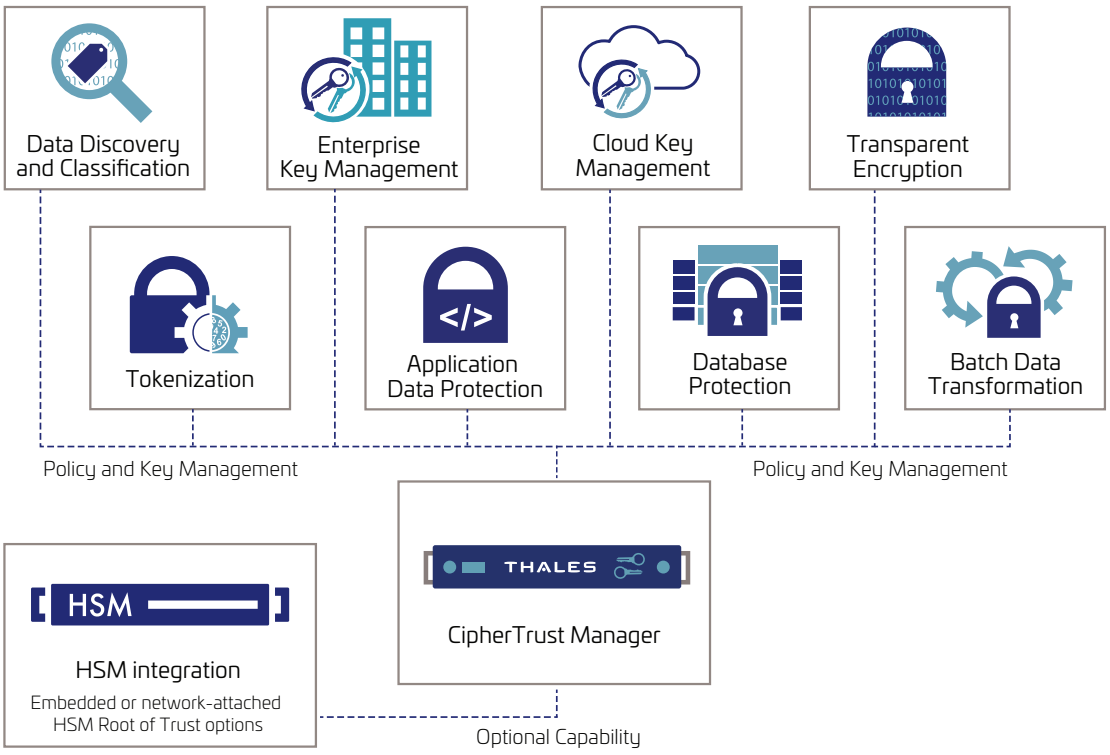
	k170v	k470v
Minimum Number of CPUs	2	4
Minimum RAM (GB)	4	16
Minimum Hard Disk (GB)	100	200
Minimum vNICs	1	2

Safety Certifications	Applicable Administrative Unit
CB Scheme	44 countries
CSA-UL	Canada/US

Emissions Certifications	
FCC Part 15, Subpart B, Class B	US
EN55032:2010, EN55024:2010,EN61000-3-2:2006 +A1:2009 +A2:2009EN61000-3-3:2008	EU
ICES-003 Issue 4 February 2004	Canada
C-TickAS/NZS CISPR 22:2009	Australia/NZ
VCCI V-3/2009.04	Japan
KN22, KN24, KC Mark	South Korea
NOM	Mexico
BIS	India

Unified management and administration across the hybrid enterprise

CipherTrust Manager minimizes capital and expense costs by providing central management of heterogeneous encryption keys, including keys generated for CipherTrust Data Security Platform products, Microsoft SQL TDE, Oracle TDE and KMIP-compliant encryption products. CipherTrust Manager features an intuitive web-based console and APIs for managing encryption keys, policies, and auditing across an enterprise.



CipherTrust Data Discovery and Classification

Data Discovery and Classification locates regulated data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, prioritizing remediation, and securing your cloud transformation.

Data Discovery and Classification provides a streamlined workflow from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

Enterprise-wide data privacy

CipherTrust Data Discovery and Classification delivers an enterprise-wide data privacy solution that is simple to deploy and scale. It provides ready-to-use templates and a streamlined workflow to help you quickly discover your regulated data across traditional and modern repositories.

Single pane of glass for clear visibility

Data Discovery and Classification provides a clear understanding of sensitive data, usage, and risks of exposure, from a single pane of glass. A centralized console with visualized data and aggregated reports enables informed decisions about data sharing, digital transformation, or prioritizing remediation.

Quick start with flexibility

Data Discovery and Classification provides a comprehensive set of built-in classification templates for commonly requested data privacy and security regulations, such as GDPR, CCPA, etc., while its flexibility easily handles custom policies based on specific patterns, algorithms and more.

Demonstrate compliance

CipherTrust Data Discovery and Classification provides detailed reports that can demonstrate to auditors compliance with various regulations and laws. Efficient scans build a strong foundation for overall data privacy and security.

Flexible deployment options

Data Discovery and Classification is available in both agent-based and agentless deployment modes. The choice enables security and IT teams to select deployment modes for optimal results and efficient cost of ownership.

Benefits

- Reduce complexity and risk with streamlined workflows unique to your organization
- Privacy officers can rapidly uncover privacy gaps, prioritize remediation, and proactively respond to regulatory and business challenges from a single pane of glass
- Build a strong foundation for overall data privacy and security through effective scans that help discover both structured and unstructured data across a diverse set of data stores
- Ensure secure third party data sharing by scanning for sensitive data and removing it, as needed, in advance

Data Discovery and Classification Technical Specifications

Data Stores

- Local storage and local memory on the host
- Network storage
  - Windows Share (CIS/SMB)
  - Unix File System (NFS)
- Databases
  - IBM DB2
  - Oracle
  - SQL
- Big Data
  - Hadoop Clusters

Type of files supported

- Databases: Access, DBase, SQLite, MSSQL MDF & LDF
- Images: BMP, FAX, GIF, JPG, PDF (embedded), PNG, TIF
- Compressed: bzip2, Gzip (all types), TAR, Zip (all types)
- Microsoft Backup Archive: Microsoft Binary / BKF
- Microsoft Office: v5, 6, 95, 97, 2000, XP, 2003 onwards
- Open Source: Star Office / Open Office
- Open Standards: PDF, HTML, CSV, TXT

Type of data identified

- Health (Australian Medicare Card, European EHIC, US Health Insurance Claim number, etc.)
- Financial (American Express, Diners Club, Mastercard, VISA card numbers, bank account number, etc.)
- Personal (name, last name, address, DOB, email, etc.)
- National ID (social security number, Spanish DNI, etc.)
- Custom information types

Pre-built templates

The solution includes a wide range of ready-to-use templates that can help you meet common regulatory and business policy needs:

- CCPA
- GDPR
- HIPAA
- PCI DSS
- PII
- PHI

Minimum RAM required

- 16GB

Network Connection

- At least 1GB

CipherTrust Enterprise Key Management

CipherTrust key management products centralize key management for CipherTrust platform applications as well as 3rd party devices, databases, cloud services and applications. Organizations gain greater command over encryption keys while increasing data security. CipherTrust key management products connect with applications through standard interfaces and deliver access to robust key management and encryption functions.

Enterprise key management solutions

CipherTrust Enterprise 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, allowing those keys to be managed with a common set of policies. CipherTrust Manager operates in the KMIP Server role for a broad range of third party applications and devices acting in the KMIP client role.

Database and Linux Key Management

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

Key Management for Proprietary Applications

For the most convenient integrations into applications that perform encryption but require centralized key management CipherTrust Manager offers developer-friendly API's that can be leveraged in a wide range of application environments. For the most performance-sensitive applications, CipherTrust Application Data Protection offers application-layer libraries implementing Java, C, C++, .NET and .NET CORE with key management "providers" for Microsoft Crypto Next-Generation (CNG) and Crypto Services Provider (CSP) plus PKCS#11.

Key Management Technical Specifications

Administration

- Secure-web, CLI, API
- Command line scripts

Key Formats for Search, Alerts, and Reports

- Symmetric encryption key algorithms: AES, ARIA
- Assymetric key algorithms
  - RSA
  - Elliptic Curve: brainpool, prime, secp

Third-Party Encryption

- Microsoft SQL TDE, Microsoft SQL Always Encrypted, Oracle TDE

API Support

- PKCS#11
- Microsoft Extensible Key Management (EKM)
- KMIP

Key Availability and Redundancy

- Secure replication of keys across multiple appliances with automated backups

Verified KMIP Integrations

HCI

- Cloudian HyperStore, VMware vSAN/VMCrypt, Nutanix, Dell EMC ECS, NetApp Cloud ONTAP, Hedvig Distributed Storage Platform, Dell EMC PowerOne, Dell EMC PowerFlex

Backup

- Commvault Data Protection Advanced

Mainframe

- Syncsort Assure Encryption for IBM i-Series

Storage

- DellEMC Data Domain, DellEMC PowerEdge, NetApp FAS, HPE Proliant/StoreEasy (iLO)*, HPE 3PAR, HPE Primera, IBM DS8000 Series

Flash Storage

- Dell EMC PowerMax, IBM , Dell EMC PowerStore

Tape Libraries

- HPE StoreEver, Quantum Scalar series

Database/Big Data

- MongoDB, IBM DB2, Oracle MySQL

*integrated via NAE-XML API

CipherTrust Cloud Key Manager

Many cloud service providers offer data-at-rest encryption capabilities. Meanwhile, many data protection best practices indicate that encryption keys be managed remote from the cloud service provider. Cloud provider "Bring Your Own Key" (BYOK) services and API's can fulfill these requirements.

Customer key control

BYOK-based customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them. Leveraging BYOK API's, CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers full lifecycle control of encryption keys with centralized management and visibility.

Key benefits

- Gain higher IT efficiency with centralized key management across multiple cloud environments, leveraging automated key rotation and expiration management
- Achieve the value of "Bring Your Own Key" services with full cloud encryption key lifecycle management
- Comply with the most stringent data protection mandates with secure key origination along with key usage logging and reporting

Enhanced IT efficiency

Capabilities supporting IT efficiency include

- Centralized access to each cloud provider from a single browser window
- Management of native cloud keys
- Automated synchronization ensures that cloud console operations are centrally visible
- Automated key rotation with support for expiring keys can save thousands of hours per year

Encryption key security

Secure key generation fulfills requirements for encryption key security utilizing CipherTrust Manager or the Vormetric Data Security Manager to create keys with up to FIPS 140-2 Level 3 security.

Compliance tools you need

Key activity logs and prepackaged reports enable fast compliance reporting. Logs may be directed to multiple syslog servers or SIEM systems.

Technical specifications

CipherTrust Cloud Key Manager is available in two editions: a standalone appliance and as a service embedded in CipherTrust Manager. Key Lifecycle management capabilities are identical between the editions.

BYOK and cloud native key management

- Create
- Upload
- Enable/Disable
- Revoke
- Delete
- Rotate
- Automated rotation and expiration
- Key metadata and policy management
- Automated cloud key vault synchronization

	Appliance	Embedded
Clouds Supported	• Azure, Azure Stack, Azure Germany and China Sovereign Clouds • Office365 • AWS • Salesforce and Salesforce Sandbox • IBM Cloud • Google Cloud CMEK	• Azure and Azure GovCloud • Office365 • AWS, AWS GovCloud, AWS China
Key Sources	• CipherTrust Manager • Vormetric Data Security Manager	• CipherTrust Manager on which embedded is operating
User Authentication	• Pass-through to cloud provider	• User management on CipherTrust Manager
Deployment Options	• VMware • Azure Marketplace • AWS • Azure Stack	• VMware • OpenStack • Azure Marketplace • Azure GovCloud • AWS • AWS GovCloud • Google Cloud • Oracle Cloud

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, granular access controls and data access logging that helps organizations meet compliance reporting and best practice requirements for protecting data.

The solution's transparent approach protects structured databases and unstructured files, across multiple cloud environments, and within big data implementations. Implementation is seamless – keeping both business and operational processes unchanged.

Meet compliance requirements

Encryption, access controls and data access logging are basic requirements or recommended best practices for almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/Hitech, GDPR and many others. CipherTrust Transparent Encryption delivers the required controls.

Scalable encryption

CipherTrust Transparent Encryption runs at the file system or volume level on a server, and is available for Microsoft Windows Server, many variants of Linux, and IBM AIX operating systems. It can be used in physical, virtual, cloud, and big data environments – regardless of the underlying storage technology. Administrators perform all policy and key administration through CipherTrust Manager.

Server-based encryption eliminates bottlenecks with both performance and scalability further enhanced by leveraging cryptographic acceleration built into CPUs, such as Intel AES-NI and IBM POWER.

Granular access controls

Granular, least-privileged access policies protect data from external attacks and privileged user misuse. Policies can be applied by users and groups from systems, LDAP/Active Directory, and Hadoop. Controls include process, file type and other parameters.

Access policies can be defined to create a permitted list of "trusted" applications to prevent any untrusted binaries (e.g. ransomware) from accessing data stores protected by CipherTrust Transparent Encryption and to prevent privileged users from accessing user data in files and databases. These access policies can block any rogue binaries from encrypting files/databases, even if the intruder has execute permissions for that binary and read/write permission to the target file that contains business critical data.

Non-intrusive, transparent deployment

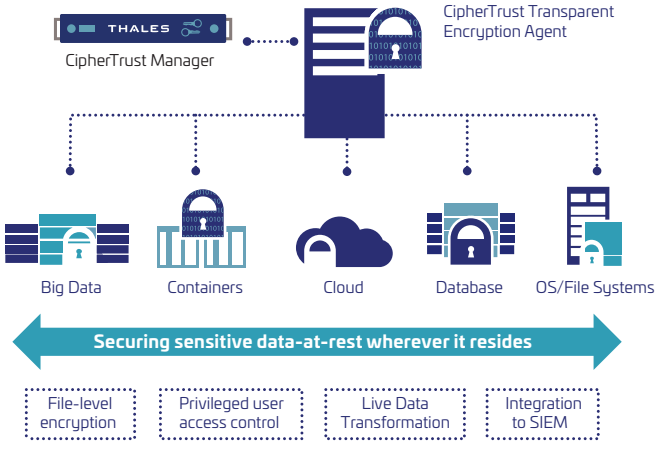
The solution requires no changes to applications, workflows, business or operational procedures.

Key benefits

- Meet compliance and best practice requirements for encryption and access control that scales
- Easy to deploy: no application customization required
- Establish strong safeguards against abuse by privileged insiders and malware using stolen credentials

Key features

- Broadest platform support in industry: Windows, Linux and AIX operating systems
- High performance encryption: Uses hardware encryption capabilities built into host CPUs - Intel, AMD AES-NI and IBM POWER AES encryption
- Logs permitted, denied and restricted access attempts from users, applications and processes
- Role-based access policies control who, what, and how data can be accessed
- Enable privileged users to perform work without access to clear-text data

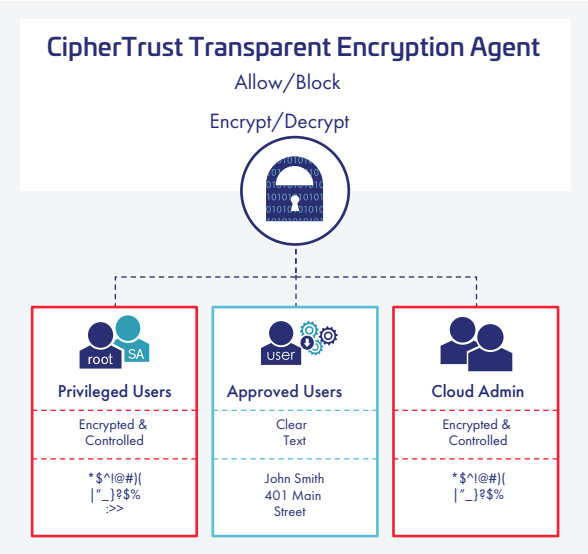


CipherTrust Transparent Encryption secures data wherever it resides

Protect data on-premises or in-cloud

Cloud data security might seem easy at first. Turning on the equivalent of full-disk encryption for a public cloud provider is simple. But it's a multi-cloud world. Managing data security across multiple public clouds and different cloud storage options quickly gets complex. CipherTrust Transparent Encryption enables you to secure your cloud data from more threats than can cloud-native encryption, with controls and keys centralized and common across multiple infrastructure as a service (IaaS) clouds. The result is lowered operational costs and data mobility between clouds.

CipherTrust Transparent Encryption protects nearly any storage mapped to IaaS environment operating systems. And with advanced data protection for Amazon S3, organizations can apply transparent encryption and access controls to sensitive data in S3 buckets. The CipherTrust Transparent Encryption solution encrypts unstructured files, semi-structured data, or structured databases before they are written to Amazon S3 buckets. The solution works in conjunction with the FIPS 140-2 up to Level 3 compliant CipherTrust Manager, assuring strong separation of key and policy management from the data. Once an S3 bucket is guarded with CipherTrust Transparent Encryption, any file deposited in it is automatically encrypted, and the data inside is rendered useless in the event of unauthorized access. With CipherTrust Transparent Encryption's support for Amazon S3, organizations can ensure that volumes of data stored in the cloud are safe and comply with the strictest security regulations while helping to close the cloud industry's most common security gaps.



Security Intelligence

CipherTrust Transparent Encryption in concert with CipherTrust Manager provides insight into file access activities. Data access logging includes detail on both authorized data access and unauthorized access attempts wherever CipherTrust Transparent Encryption is operating. Information provided also includes actions of security administrators – another item required for compliance audit purposes.

Security Intelligence logs are forwarded to SIEM systems via SYSLOG or CEF among other protocols to speed up threat detection.

Data sets can also be used to create access pattern baselines which can then be used to rapidly identify threats represented by behavior deviating from baseline.

CipherTrust Transparent Encryption Technical Specifications

Encryption Algorithms and Capabilities
- AES, ARIA

Extension Licenses
- Live Data Transformation

Platform Support
- Microsoft: Windows Server 2019, 2016 and 2012
- Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu
- UNIX: IBM AIX

Database Support
- IBM DB2, Microsoft SQL Server, Microsoft Exchange Data Availability Group (DAG), MySQL, NoSQL, Oracle, Sybase and others

Application Support
- Transparent to all applications, including SAP, SharePoint, custom applications and more

Big Data Support
- Hadoop: Cloudera, IBM
- NoSQL: Couchbase, DataStax, MongoDB
- SAP HANA

Encryption Hardware Acceleration
- AMD and Intel AES-NI
- IBM POWER9 cryptographic coprocessor

Agent Certification
- FIPS 140-2 Level 1

Cloud Support
- AWS: EBS, EFS, S3, S3I, S3 Glacier
- AZURE: Disk Storage, Azure Files
- GCP: Persistent Disk, Local SSD, Filestore

CipherTrust Transparent Encryption Extensions and Additions

CipherTrust Live Data Transformation

Data-at-rest encryption deployment and management can present challenges during initial encryption or when rekeying data that has already been encrypted, requiring either planned downtime or data cloning and synchronization. Live Data Transformation for CipherTrust Transparent Encryption enables encryption and rekeying with unprecedented uptime and administrative efficiency.

Zero-downtime encryption and key rotation

Administrators can encrypt data without downtime or disruption to users, applications or workflows. While encryption is underway, users and processes continue to interact with databases or file systems as usual.

Security best practices and regulatory mandates require periodic key rotation. Live Data Transformation addresses these requirements with speed and efficiency through online key rotation and data rekeying.

Live Data Transformation provides resource management capabilities to balance between encryption and business demands. An administrator can define a rule specifying that, during business hours, encryption can only consume 10% of system CPU, while on nights and weekends, encryption can consume 70% of CPU. Similar controls are available for I/O operations.

Live Data Transformation offers faster backup and archive recovery. 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.

Live Data Transformation Technical Specifications

Operating System Support

- Microsoft: Windows Server 2019, 2016 and 2012
- Linux: Red Hat Enterprise Linux 7 and 8, SuSE Linux Enterprise Server 12 and 15

Cluster support

- Microsoft Cluster: File Cluster, SQL Server Cluster

Database support

- IBM DB2, IBM Informix, Microsoft SQL Server, Oracle, Sybase and others

Big Data Support

- Cassandra, CouchBase, Hadoop, MongoDB, SAP HANA

Backup/Replication Support

- DB2 backup, NetBackup, NetWorker, NTBackup, Oracle Recovery Manager (RMAN), Windows Server Volume Shadow Copy Service (VSS)

CipherTrust Transparent Encryption for SAP HANA

CipherTrust Transparent Encryption safeguards SAP HANA data enabling enterprises to meet rigorous security, data governance, and compliance requirements. The solution enforces strong data encryption on all SAP HANA data and log partitions and protects and controls access to the SAP HANA Persistence layer. The solution can be quickly deployed and requires no changes to SAP HANA or the underlying database or hardware infrastructure. Further, SAP has reviewed and qualified CipherTrust Transparent Encryption as suitable solution for SAP HANA 2.0 environments.

CipherTrust Tokenization

Tokenization reduces the cost and effort required to comply with security policies and regulatory mandates such as the European Union's Global Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS). CipherTrust Tokenization offers application-level tokenization services in two convenient solutions that deliver complete customer flexibility: 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.

Vaultless Tokenization

CipherTrust Vaultless Tokenization protects data at rest while its policy-based Dynamic Data Masking capability protects data in use. A RESTful API in combination with centralized management and services enables tokenization implementation with a single line of code per field. Vaultless Tokenization is provided by dedicated, distributed-cluster-capable Tokenization Servers, offering full separation of duties. Tokenization management and configuration including an operational dashboard with convenient tokenization configuration workflows occurs in a graphical user interface.

Dynamic Data Masking. Policies define whether a tokenized field is returned fully or partially masked based on user identification controlled by an AD or LDAP server. For example, the policies could enable customer service representatives to see only the last four digits of credit card numbers, while account receivables staff could access the full credit card number.

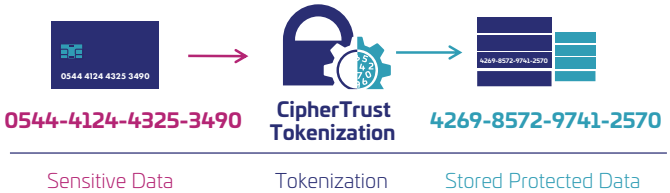
Non-disruptive. Format preserving tokenization protects sensitive data without changing the database schema.

Vaulted Tokenization

CipherTrust Vaulted Tokenization also offers non-disruptive format-preserving tokenization with a wide range of existing formats and the ability to define custom tokenization formats. Vaulted Tokenization provides a high level of security for highly sensitive data, and instances of it may be installed on a per-server basis or installed as a web service supporting multiple clients.

Fast integration

CipherTrust Tokenization solutions are rapidly integrated with minimal software engineering, leveraging standard protocols and environment bindings.



Vaultless Tokenization Technical Specifications

Tokenization capabilities:

- Format-preserving tokens with irreversible option
- Random tokens data length up to 128K
- Date tokenization
- Unicode UTF-8 character set support enable data tokenization in almost any language
- Luhn checking option for FPE and random tokens

Dynamic data masking capabilities:

- Policy based, number of left and/or right characters exposed, with customizable mask character
- Authentication with Lightweight Directory Access Protocol (LDAP) or Active Directory (AD)

Deployment Form Factors and Options:

- Open Virtualization Format (.OVA) and International
- Organization for Standardization (.iso)
- Microsoft Hyper-V VHD
- Amazon Machine Image (.ami)
- Microsoft Azure Marketplace
- Google Cloud Platform

System requirements:

- Minimum hardware: 4 CPU cores, 16–32 GB RAM
- Minimum disk: 80GB

Application integration:

- RESTful APIs

Performance:

- More than 1 million credit card size tokenization transactions per second, per token server (using multiple threads and batch (or vector) mode) on a 32-core server (dual-socket Xeon E5-2630v3) with 16 GB RAM

Vaulted Tokenization Technical Specifications

Tokenization capabilities:

- Format-preserving tokens
- Random or Sequential token generation
- Purge specific tokens on demand, equivalent to purging original data
- Masked: Last four, First six, First two, etc.
- Fixed length and width masking
- Customer defined custom formats
- Regular expressions (Java style)

Supported Token Vault Databases

- Microsoft SQL Server
- Oracle
- MySQL
- Cassandra

Application integration

- RESTful APIs
- Java
- .NET

CipherTrust Application Data Protection

Overview

CipherTrust Application Data Protection offers DevSecOps-friendly software tools for key management operations, as well as application-level encryption of sensitive data. The solution is flexible enough to encrypt nearly any type of data passing through an application. Protecting data at the application layer can provide the highest level of security, as it can take place immediately upon data creation or first processing, and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy. CipherTrust Application Data Protection can be deployed in physical, private or public cloud infrastructure to secure data even when it is migrating from one environment to another, without any modifications to existing encryption or data processing policies.

CipherTrust Application Data Protection is deployed with CipherTrust Manager, an architecture that centralizes key and policy management across multiple applications, environments, or sites. The combined solution provides granular access controls that separate administrative duties from data and encryption key access. For example, a policy can be applied to ensure that no single administrator can make a critical configuration change without additional approval.

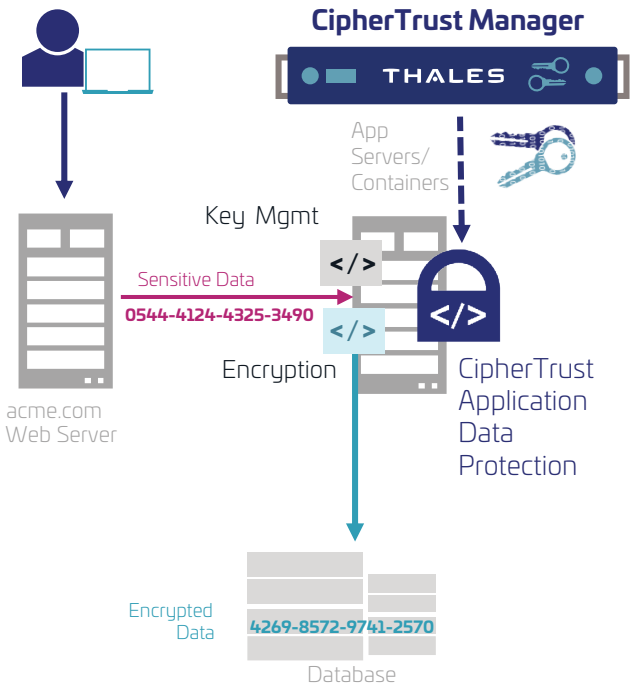
CipherTrust Application Data Protection features built-in, automated key rotation, and offers a wide range of cryptographic operations including encryption, decryption, digital signing and verification, secure hash algorithms (SHA), and hash-based message authentication code (HMAC).

CipherTrust Application Data Protection is rich in function and provides both development and, and operational flexibility:

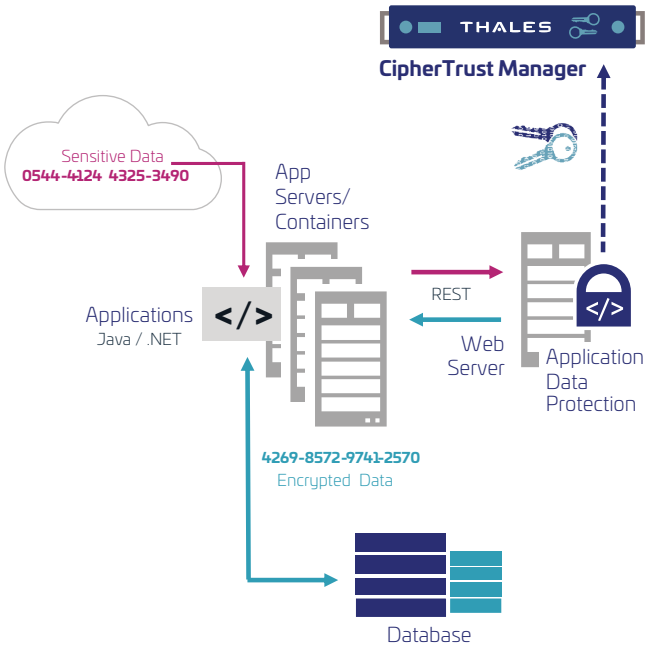
Functional richness is delivered in the form of built-in server health checking and failover coupled with multi-tiered load balancing and built-in key rotation.

Development flexibility is delivered with REST, C, .Net Core, Net and Java cryptographic libraries to enable creation of crypto applications for the widest range of programming skills.

Operational flexibility is twofold:
First, a broad range of cryptographic providers are available including native C, PKCS#11, the Cryptographic Service Provider (CSP) and Crypto Next Generation (CNG) Providers for Windows and the Java Crypto Engine (JCE).



CipherTrust Application Data Protection with Installable Libraries

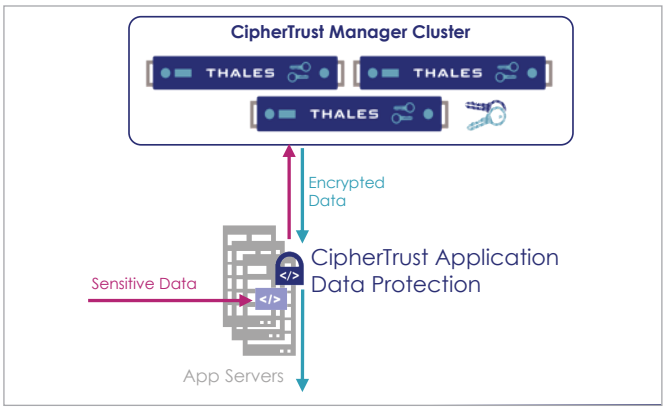


CipherTrust Application Data Protection installed as a Web Service

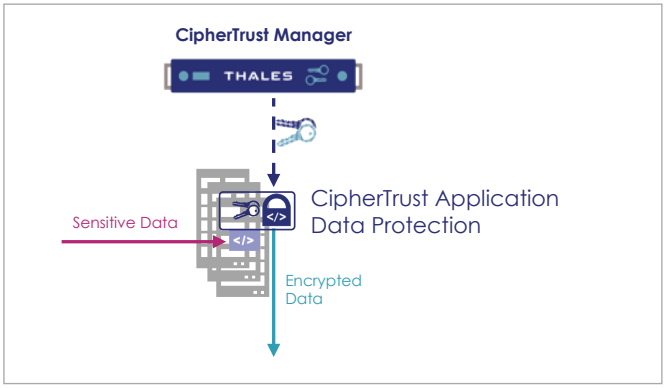
Second, **encryption operational flexibility** is delivered by the choice, for the libraries or Web Services edition of the product, to encrypt locally or on CipherTrust Manager, without changing any code.
The choice is implemented with a simple configuration change.

Where to encrypt involves choices and potential benefits:

- Encryption on CipherTrust Manager offers security, performance, and scalability benefits, and ensures that keys never leave the trusted CipherTrust Manager for the highest level of security. Offloading encryption from application servers can enable them to perform better. And, embedded in CipherTrust Application Data Protection libraries are load-balancing mechanisms that enable encryption load to be spread across a cluster of CipherTrust Managers.



- Encryption on the application server can provide potentially higher performance for certain types of encryption workloads. In contrast to open-source solutions, keys are encrypted in memory when not in use, and scattered in memory when in use. Both mechanisms secure crucial encryption keys from abuse.



CipherTrust Application Data Protection in concert with CipherTrust Manager provides a single interface for logging, auditing, and reporting access to protected data and encryption keys.

Rich Encryption Ecosystem

In addition to the key management integrations discussed above, CipherTrust Application Data Protection has integrations for Microsoft Crypto Next Generation (CNG), Microsoft Crypto Service Provider (CSP), Microsoft Online Certificate Status Protocol (OCSP), Hashi Vault, HortonWorks, Apache HTTP and NGINX Servers, Lieberman ERPM, and many others.

Benefits

- Centralized key management, freeing developers from complex and risky key management stores
- Strengthen security and ensure compliance
- Leverage the cloud with utmost security
- Accelerate security application development
- Optimize application server performance
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and cloud vendors
- Key management for a broad range of native encryption solutions

Application Data Protection Technical Specifications

Development Libraries and APIs
- Java, C, and C# for .NET Core and .NET
- KMIP standard
- XML open interface
- Web services: REST

Crypto Service Providers and Supported OS's

C provider
- Windows
- Linux
- AIX
- MacOS

KMIP Server / Provider
- On CipherTrust Manager

PKCS#11 provider
- Windows Server
- Linux
- AIX
- Solaris

Java Crypto Extension Provider
- Windows Server
- Linux
- Solaris
- HP-UX
- AIX

CSP and CNG Providers
- Windows Server 2008 and up

Encryption Algorithms
- 3DES, AES 256 (CBC and XTS), SHA 256, SHA 384, SHA 512, RSA 1024, RSA 2048, RSA 3072, RSA 4096, ECC
- Format-preserving: FF1/FF3, Tokenization

Web Application Servers
- Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, SAP NetWeaver, Sun ONE, and more

Cloud and Virtual Infrastructures
- Works with all major cloud platforms, including AWS, Azure, IBM Cloud, Google and VMware

CipherTrust Database Protection

Overview

CipherTrust Database Protection products provide 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 Database Protection and CipherTrust Teradata Database Protection offer convenient choices in database protection and both leverage CipherTrust Manager for centralized key management. Further, configuration of CipherTrust Database Protection is done centrally on the CipherTrust Manager console.

The solutions enable sensitive data fields in databases to be efficiently protected and secured. Both solutions are transparent to applications and business processes, requiring no changes. And both are cloud-friendly. For efficiency, both products offer mechanisms either to encrypt locally for performance or in CipherTrust Manager to ensure that encryption keys never leave the secure enclave, without changing any code. The choice is implemented with a simple configuration change.

Database Protection Technical Specifications

Supported Databases

- Oracle
- Microsoft SQL Server
- IBM DB2
- Teradata Database

Supported Platforms

- Microsoft Windows
- Linux
- Solaris
- HP-UX
- AIX

Encryption Algorithms

- FPE (FF1, FF3), AES, 3DES, RSA, ECC

CipherTrust Database Protection

CipherTrust Database Protection encrypts data, leveraging database views and triggers to ensure that access to non-encrypted and encrypted fields remains transparent to applications. Key granularity is on a per-field basis.

Deployment and initial use

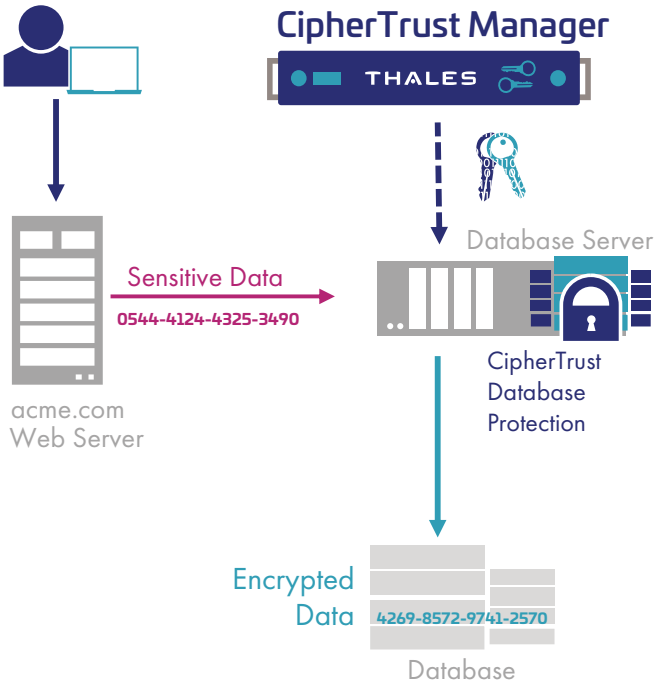
CipherTrust Database Protection is installed on each database server. It can be installed manually or in a silent mode, or, for example, with Chef recipes.

Once installed, software on the database server is securely linked to a CipherTrust Manager for access to keys, and, for some configurations or databases, encryption and decryption services.

Installation is usually followed by a data migration process involving selection of data, typically columns, to encrypt, defining database table, view, and trigger design, and finally bulk data encryption.

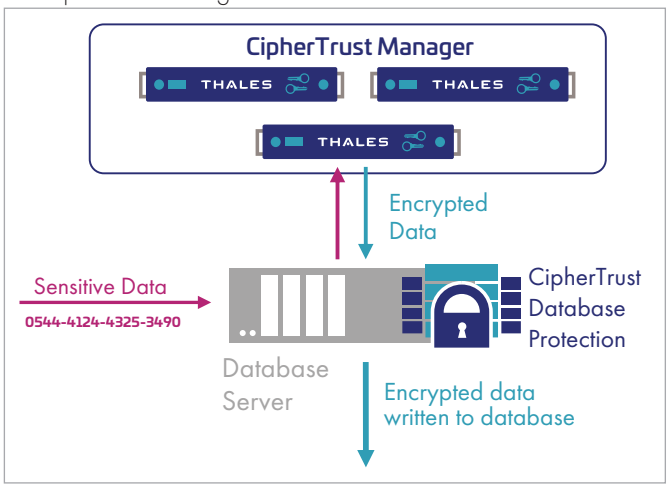
From then onward, the triggers and views enable

- new data to be encrypted
- database reads to be decrypted for permitted users
- database updates to be encrypted with full transparency to users and workflows.

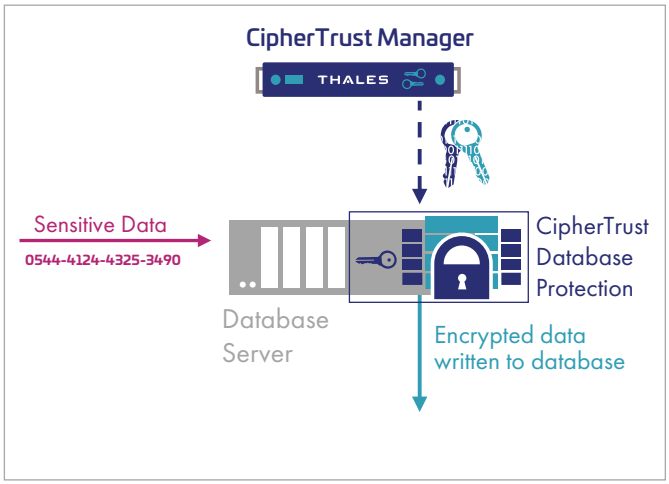


Where to encrypt when using CipherTrust Database Protection involves choices and potential benefits:

- Encryption on CipherTrust Manager offers security, performance, and scalability benefits, and ensures that keys never leave the trusted CipherTrust Manager for the highest level of security. Offloading encryption from database servers can enable them to perform better. And, embedded in CipherTrust Database Protection are load-balancing mechanisms that enable encryption load to be spread across a cluster of CipherTrust Managers.



- Encryption on the database server can provide potentially higher performance for certain fields of database encryption. In contrast to open-source solutions, keys are encrypted in memory when not in use, and scattered in memory when in use. Both mechanisms secure crucial encryption keys from abuse.



CipherTrust Teradata Protection

CipherTrust Protection for Teradata Database simplifies the process of securing sensitive columns in the Teradata Vantage SQL Database. The solution offers both traditional encryption and NIST-approved format-preserving encryption (FPE) capabilities, enabling protection of fields without altering their format to minimize the potential impact of data protection on associated applications and workflows and avoid the increased storage requirements of conventional encryption approaches. And the solution offers dynamic data masking, enabling different levels of decryption and presentation of data to specific users.

Streamline encryption deployment and usage

The solution reduces potential complexity arising from data protection for Teradata Vantage SQL as user-defined function (UDF) in the database engine, enabling data access to be controlled separate from database users and administrators.

Security administrators specify data access profiles defining encryption methods and user-specific alllow- and deny-lists. The solution also enables the use of different encryption keys per database column, and then binding unique keys to one or more Teradata Vantage Database users. Specific deny behaviors are also available on a per-user basis. Further, once data is encrypted, even if UDF's are disabled administratively, data remains protected.

Benefits

- Boost security without compromising the value of big data analytics
- Establish protections against cyber attacks and abuse by privileged users
- Fast, convenient deployment and configuration

Technical Specifications

Supported Databases
- Teradata Database, minimum version 16.2

Supported Platforms
- SUSE Linux Enterprise Server (SLES) minimum version 11 SP3

Encryption Algorithms
- AES, FPE (FF1, FF3)

Maximum Column Widths
- ASCII—16KB, Unicode—8KB

Encryption Controls
- Identity-based access per column
- Dynamic masking based on identity
- Allow/Deny access controls

Encryption Key Sources
- CipherTrust Manager

CipherTrust Batch Data Transformation

Static Data Masking

Static Data Masking transforms selected data to unreadable forms in order to utilize data sets while preventing misuse of sensitive data.

CipherTrust Batch Data Transformation offers high-performance data masking with centralized encryption key management, leveraging CipherTrust Application Data Protection and CipherTrust Tokenization to protect vast quantities of data quickly.

Static Data Masking has many use cases. These four begin with "masking sensitive data".

1. Prior to sharing data with third parties.

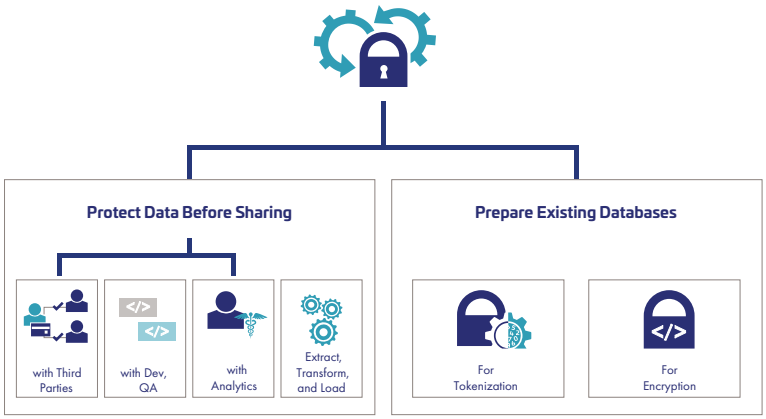
2. In databases shared with development, QA, R&D or analytics.

3. Before adding a data set to a big data environment.

4. In advance of extract, transform and load (ETL) operations.

Other use cases include

- Preparing a database for a tokenization or encryption deployment
- Rekeying an encrypted column of data after key rotation



CipherTrust Batch Data Transformation for High-Volume Flexible Data Masking, Tokenization and Encryption

Key benefits

- Secure, cost-effective static data masking with centralized data encryption keys sourced from up to FIPS 140-2 Level 3 sources
- Enable database sharing with reduced risk
- Accelerates protection of existing data following deployment of CipherTrust Data Discovery and Classification
- Static data masking where you need it. Deploy on-premises or in the cloud, or hybrid deployment.

Technical specifications

Data Transformation Options:

- Tokenization, Data Encryption
- Formatting preserving alpha/numeric

Policy File Options:

- Specific action for each individual column transformation – encrypt, decrypt, tokenize, de-tokenize and re-key
- Easy to apply encryption without the need for application changes
- Flexible key management options – keys in CipherTrust Manager or server, multiple key support

Data Security Platform Requirements

- Key sources: CipherTrust Manager, Vormetric Data Security Manager, KeySecure Classic
- Pre-requisite components: tokenization requires CipherTrust Tokenization Server deployment and license; encryption requires either CipherTrust Application Data Protection or Vormetric Application Encryption and license

Hardware and Operating System Requirements:

- Processor with 4 cores, 16GB RAM (minimum)
- Java Runtime Environment (JRE)
- Windows Server 2012 minimum
- Linux – RedHat, CentOS, Ubuntu and SUSE

THALES

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales Luna Backup HSM

Thales Luna Backup Hardware Security Modules (HSMs) are widely used by enterprise, financial institutions and government to securely backup high value cryptographic key material. This accessory to Thales Luna Network and PCIe HSMs enables you to reduce risks, maintain SLAs, and ensure regulatory compliance, ensuring your critical data is securely stored offline.

Secure backup

Maintaining keys in hardware throughout their life-cycle is a best practice mandated by system security auditors and certification bodies responsible for attesting to the security status of cryptographic systems.

The Luna Backup HSM ensures your sensitive cryptographic material remains strongly protected in hardware even when not being used. You can easily backup and duplicate keys securely to the Luna Backup HSM for safekeeping in case of emergency, failure or disaster. The remote backup capabilities allow administrators to securely replicate sensitive cryptographic key material to other Luna HSMs. With a single Luna Backup HSM, an administrator can backup and restore keys to and from up to 100 partitions.

The Luna Backup HSM provides the same level of security as the Luna Network and PCIe HSMs in a convenient, small, low cost form factor. It provides an additional layer of hardware-based security.

Features & Benefits:

Highest Security & Compliance:

- Keys always remain in FIPS-validated*, intrusion-resistant, tamper-evident hardware
- Remote management, backup and restore for quick disaster recovery
- Multi-person MofN with multi-factor authentication for increased security and strong separation of duties
- High-assurance delivery with secure transport mode

* in progress

High assurance key protection

By its very name, HSM implies hardware. As such, most security professionals assume that all HSMs actually store cryptographic keys in hardware, as Luna HSMs do by default. In fact, while other leading HSMs generate their keys in hardware, they actually store the cryptographically wrapped keys on an application server. These keys, residing in software, can be easily detected—creating an additional attack surface.

The advantages of hardware are the key reasons why the world's largest enterprises and government organizations trust Luna HSMs to guard more digital identities and interbank fund transfers than any other HSM in the world.

Built for ease of use

- Portable, handheld, small form factor device
- Host powered USB – no need for a power adaptor
- LCD touch screen enables quick review of the HSM status including partitions, firmware, megabytes remaining, and more
- Easy setup – up and running in minutes

Technical specifications

Operating System Support

- Windows, Linux

Client

- Thales Luna Client

Security Certifications

- FIPS 140-2 Level 3*

Physical Characteristics

- Dimensions: 5.7" x 3.4" x 0.91" (144.7mm x 86.4mm x 23.1mm)
- Weight: 400g
- 4.7" LCD touch screen
- Input Voltage: 100 - 240V, 50 - 60Hz

Input 5VDC 2 A for USB power

- Power Consumption: 6.4W maximum, 4.0W typical
- Temperature: operating 0°C – 40°C, storage -20°C – 70°C
- Relative Humidity: 20% to 95% (38°C) non-condensing

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1] (in progress)
- TAA

Storage

- Up to 100 partitions

Host Interface

- USB 3.0 Type C connector

Reliability

- MTBF: 564181 hrs @40C, Telcordia SR-332, Issue C

Supported Versions

- Backup and restore from multiple HSMs including Luna HSM 7 and Luna Cloud HSM

Available models

Choose from the following Luna Backup HSM models:

- **HSM B700**, 32MB of storage space
- **HSM B750**, 128MB of storage space
- **HSM B790**, 256MB of storage space

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.

* in progress

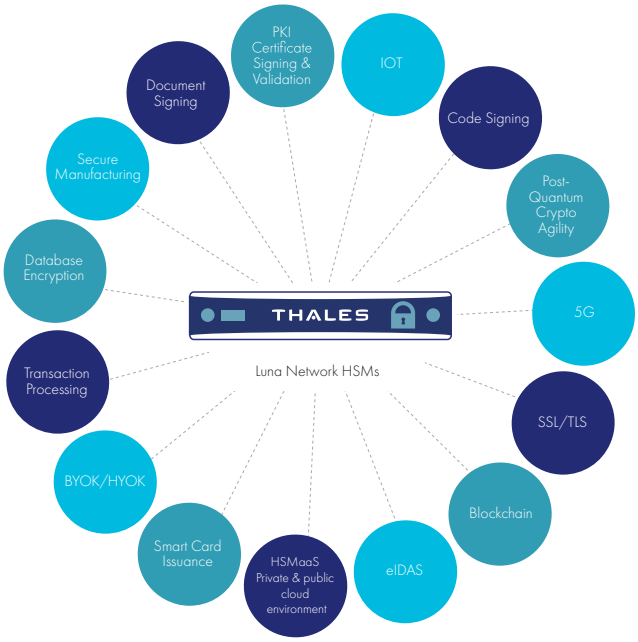
cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales Luna Network HSM

Secure your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in Thales Luna Network Hardware Security Modules (HSMs) - high-assurance, tamper-resistant, network-attached appliances offering market-leading performance.

Contact us to learn how you can integrate Luna Network HSMs into a wide range of applications to accelerate cryptographic operations, secure the crypto key lifecycle, and provide a root of trust for your entire encryption infrastructure.



What you need to know:

Superior Performance:

- Meet your high throughput requirements with over 20,000 ECC and 10,000 RSA operations per second for high performance use cases
- Lower latency for improved efficiency

Highest Security & Compliance:

- Keys always remain in FIPS-validated, tamper-evident hardware
- Meet compliance needs for GDPR, eIDAS, HIPAA, PCI-DSS, and more

- De facto standard for the cloud
- Multiple roles for strong separation of duties
- Multi-person MofN with multi-factor authentication for increased security
- Secure audit logging
- High-assurance delivery with secure transport mode
- High quality keys through external Quantum RNG seeding
- Securely backup and duplicate keys in hardware with Luna Backup HSM or to the cloud with Data Protection on Demand for redundancy, reliability and disaster recovery

Reduce Costs & Save time:

- Remotely manage HSMs - no need to travel
- Reduced audit and compliance costs and burdens
- Automate enterprise systems to manage HSMs via REST API
- Efficiently administer resources by sharing HSMs amongst multiple applications or tenants
- Flexible partition policies to meet your key management and compliance needs
- Increased portability, greater efficiency and less overhead using Luna Client in a container
- Functionality Modules
  - Extend native HSM functionality
  - Develop and deploy custom code within the secure confines of the HSM

Technical specifications

Supported Operating Systems

- Windows, Linux, Solaris, AIX
- Virtual: VMware, Hyper-V, Xen, KVM

API Support

- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
- REST API for administration

Cryptography

- Full Suite B support
- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more
- Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST, and more
- Hash/Message Digest/HMAC: SHA-1, SHA-2, SHA-3, SM2, SM3, SM4 and more
- Key Derivation: SP800-108 Counter Mode
- Key Wrapping: SP800-38F
- Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG
- Digital Wallet Encryption: BIP32
- 5G Cryptographic Mechanisms for Subscriber Authentication: Milenage, Tuak, and COMP128

Security Certifications

- FIPS 140-2 Level 3 – Password and Multi-Factor (PED)
- Common Criteria EAL4+ (AVA_VAN.5 and ALC_FLR.2) against the Protection Profile EN 419 221-5
- Qualified Signature or Seal Creation Device (QSCD) listing for eIDAS compliance
- Singapore NITES Common Criteria Scheme

Host Interface

- 2 options: 4 Gigabit ethernet ports with Port Bonding, or 2 x 10G fiber network connectivity and 2 x 1G with Port Bonding
- IPv4 and IPv6

Physical Characteristics

- Standard 1U 19in. rack mount appliance
- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Weight: 28lb (12.7kg)
- Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 100W maximum, 84W typical
- Heat Dissipation: 376BTU/hr maximum, 287BTU/hr typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Safety & Environmental Compliance

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC Mark
- RoHS2, WEEE
- TAA
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

Reliability

- Dual hot-swap power supplies
- Field-serviceable components
- Mean Time Between Failure (MTBF) 171,308 hrs

Management & Monitoring

- HA disaster recovery
- Backup and restore hardware to hardware on-premises or in the cloud
- SNMP, Syslog

Available models

Choose from two series of Luna Network HSMs, each one with 3 different models to fit your requirements.

Luna A Series:

Password Authentication for easy management.

Standard Performance **A700**	Enterprise Performance **A750**	Maximum Performance **A790**
2 MB Memory	16 MB Memory	32 MB Memory
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**Performance:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**Performance:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna S Series:

Multi-factor (PED) Authentication for high assurance use cases.

Standard Performance **S700**	Enterprise Performance **S750**	Maximum Performance **S790**
2 MB Memory	16 MB Memory	32 MB Memory
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
Performance: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**Performance:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**Performance:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = transactions per second

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

thalesgroup.com

Thales Luna PIN Entry Device (PED)

The Thales Luna PIN Entry Device (PED) enables you to manage the security administration functions on a Thales Luna hardware security module (HSM). This PED device provides the flexibility to administer an HSM locally or remotely, while still maintaining the highest levels of security through FIPS 140-2-validated two-factor authentication.

Secure HSM Management

To manage an HSM located at a remote site, the PED simply connects to any Windows-based workstation via a USB cable. Mutual authentication between the remote PED and the HSM provides a secure, encrypted tunnel that protects the confidentiality and integrity of the data being exchanged. Remote PED Software running on the workstation acts as a communications bridge between the PED and the Luna HSM over a network socket.

The Luna PED can also be connected directly to the HSM for local management of security functions.

Thales Luna PED Remote Management Highlights

Secure Two-Factor Authentication

The Luna PED employs two-factor authentication, providing full separation of security administration functions. To establish a secure connection, the Remote PED key is inserted into the Luna PED. To complete authentication, a unique PIN is entered using the PED keypad. Once secure communications have been established, all interactions between the Luna HSM, Luna PED, and PED keys are performed in exactly the same way as they would be if the PED were locally connected to the HSM. The trusted path extends from the Luna HSM directly to the PED, with no network air gaps on any device in between, ensuring critical PED key data remains confidential.

Benefits

Easy Management

- Remote and local management of Luna HSMs
- Secure audit logging
- Manage multiple HSMs with a single PED for reduced total cost of ownership
- Efficiently administer remote HSMs, saving time and travel costs
- USB-powered PED for easy set up (no need for a power adapter)

Highest Security

- Tamper-evident seal
- Multi-person MofN with multi-factor authentication for increased security and role separation

Centralized HSM Management

The Luna PED allows the security administrator to centrally manage administrative functions on an HSM by simply inserting the required key and entering the secret PIN into the PED. After establishing a common PED role between the Luna HSM and the remote workstation, all HSM PED operations can be performed remotely including:

- HSM initialization and re-initialization
- Role creation including Security Officer (SO), Partition SO, Crypto Officer, Crypto User, and Domain

Highly Secure

All communication between the Luna PED and the Luna HSM is transmitted within an AES-256 encrypted channel using session keys based on secrets shared out-of-band via the remote PED role. The Advanced Encryption Standard (AES) provides a significant increase in the level of protection to fortify defenses against today's most common hacking threats.

Technical Specifications

The Luna PED kit includes:

- Luna PED device
- PED Cable for connecting direct to HSM
- USB cable (power adapter not required)

Operating Systems

- Windows 7
- Windows 10

Physical Characteristics

Connectivity

- USB spec 2.0
- Plug-and-play support for Windows

Dimensions

- 6.65"x4"x1"

Power Dissipation

- 0.65W typical

Regulatory Standards Certification

- CE/C-UL/FCC
- FCC 47 CFR Part 15, Subpart B
- RoHS 2011/65/EU

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.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com

cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales ProtectServer 3 Network HSMs

ProtectServer 3 External
ProtectServer 3+ External

Thales ProtectServer 3 Network Hardware Security Modules (HSMs) are security hardened network crypto servers designed to protect cryptographic keys against compromise, while providing encryption, signing and authentication services to secure sensitive applications.

ProtectServer 3 External HSM

ProtectServer 3+ External HSM

Highly secure

ProtectServer Network HSMs include a cryptographic module performing secure cryptographic processing in a high assurance fashion. The appliances feature heavy-duty steel cases with tamper-protected security that safeguard against physical attacks, and deliver the highest levels of physical and logical protection to the storage and processing of highly sensitive information such as cryptographic keys, PINS, and other data. Secure storage and processing means cryptographic keys are never exposed outside the HSM in clear form, offering customers a level of security unavailable from software alternatives, while providing a certified level of confidentiality and integrity that meets the security demands of industry organizations.

Flexible programming

ProtectServer HSMs offer a unique level of flexibility for application developers to create their own firmware and execute it within the secure confines of the HSM. Known as functionality modules, the toolkits provide a comprehensive facility to develop and deploy custom firmware. A full-featured software emulator rounds out the flexible development tools, enabling developers to test and debug

Benefits

Performance

- 3500 RSA-1024 signatures / sec

Security

- FIPS 140-2 Level 3 validated*
- Physical tamper protection
- True Random Number Generation
- Smartcard backup of key material

Reliability

- High quality components

Easy Management

- Intuitive GUI
- In-field secure upgrade
- Remote management

Interoperability

- ANSI X9 TR-31 Key Block Support

custom firmware from the convenience of a desktop computer. This emulator also serves as an invaluable tool to test applications without the need to install a ProtectServer HSM. When ready, a developer simply installs the HSM and redirects communication to the hardware — no software changes are necessary.

Easy management

The intuitive graphic user interface (GUI) simplifies HSM device administration and key management using easy-to-understand navigation and user interaction. Urgent and time-critical management tasks — such as key modification, addition, and deletion — can be securely performed from remote locations, reducing management costs and response times.

ProtectServer 3+ HSM

In addition to the features and functionality provided by ProtectServer 3 HSM, ProtectServer 3+ HSM employs dual swappable AC power supplies to help high-availability data centers protect against power failures, and enables business continuity by providing the ability to connect the appliance to two separate power sources to safeguard against the possible malfunction of one of the sources. This provides the necessary flexibility to perform maintenance on or replace a failed power supply or power feed with the assurance that your device will continue to operate.

High performance and scalability

ProtectServer Network HSMs perform rapid processing of cryptographic commands. Specialized cryptographic electronics — including a dedicated data cipher micro-processor, memory, and a true Random Number Generator (RNG) — offload the cryptographic processing from the host system, freeing it to respond to more requests.

ProtectServer Network HSMs are available in a broad range of symmetric and asymmetric cryptographic performance levels to meet a wide variety of security application processing requirements, with speeds up to 3500 RSA-1024 signature operations per second. The included dual-network interface optionally enables the HSMs to be integrated on the same or different subnets, and to be shared between different networks in order to protect multiple business domains or provide redundancy within a single network.

In addition, high levels of scalability, reliability, redundancy, and increased throughput can be easily achieved as there is no restriction on the number of HSMs that can work in unison, or the number of keys that can be managed.

Convenience

Smart cards provide the highest security and administrative convenience for secure backup, recovery, and transfer of cryptographic keys. Upgrades can be cost-effectively performed at the in-field location, avoiding the expense of returning the product to the service location. ProtectServer HSMs also support key component entry via a compatible PIN pad.

Multi-factor authentication

ProtectServer HSMs support multi-factor authentication. This authentication scheme adds another layer of security by requiring both the memorized token PIN and a 6-digit number randomly generated by the 110 OTP Token.

Technical specifications

Available models:

- PSE 3 available in PL25, PL220, and PL3500 performance models
- PSE 3+ available in PL3500 performance model only

Operating Systems

- Windows, Linux

Cryptographic APIs

- PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL

Cryptography

- Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519) with named, userdefined and Brainpool curves, and more
- Symmetric: AES, AES-GCM, AES-CCM, AES-GMAC, Triple DES, DES, CAST 128, RC2, RC4, SEED, ARIA plus others
- Hashing: SHA-1, SHA-2, SHA-3, MD5, MD2, RIPEMD 128, RIPEMD 160, DES MDC2 PAD1 and more
- Message Authentication Codes: SHA-1, SHA-2, SHA-3, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC, CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB MAC, DES30x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC, ARIA MAC, VISA CVV
- Digital Wallet Encryption: BIP32
- 5G Cryptographic Mechanisms for Subscriber Authentication: MILENAGE and TUAK
- ANSI X9 TR-31 Key Block Support for interoperability

Physical Characteristics

- Rack Mountable
  - Standard 1U 19" rack mount appliance
- Dimensions
  - 17.20" x 9.84" x 1.73" (437 mm x 270 mm x 44 mm) (PSE 3)
  - 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm) (PSE 3+)
- Weight
  - 6.83lb (3.1 kg) (PSE 3)
  - 28lb (12.7kg) (PSE 3+)
- Input Voltage
  - 100-240V, 50-60Hz (PSE 3)
  - 100-240V, 50-60Hz (PSE 3+)
- Power Consumption
  - 90W maximum, 58W typical (PSE 3)
  - 100W maximum, 84W typical (PSE 3+)
- Temperature
  - Operating 0°C to 35°C, storage -20° to 60°C
- Relative Humidity
  - 5% to 85% (38°C) non-condensing (PSE 3)
  - 5% to 95% (38°C) non-condensing (PSE 3+)

Host Interface

- 2 Gigabit Ethernet ports with Port Bonding (PSE 3)
- 4 Gigabit Ethernet ports with Port Bonding (PSE 3+)
- IPv4 and IPv6

Security Certifications

- FIPS 140-2 Level 3*

Management and Monitoring

- High Availability (HA) / Work Load Distribution (WLD)
- SNMP, Syslog
- Backup/Restore

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

Reliability

- Dual hot-swap power supplies (PSE 3+)
- Mean Time Between Failure (MTBF) 165637 hours (PSE 3)
- Mean Time Between Failure (MTBF) 171,308 hours (PSE 3+)

* pending

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us