thalescpl.com

THALES

SafeNet KeySecure

Overview

Centrally manage your encryption keys and ultimately own your data with SafeNet KeySecure, the industry leading enterprise key management platform. Regardless of its location, be it stored in a database, file server, application, traditional or virtualized data center, or public cloud environment, your sensitive data is secure from compromise.

Select from flexible options spanning FIPS 140-2 Level 3 or 1 validated hardware appliances. Supporting a broad encryption ecosystem— encompassing both Thales and a diverse range of third-party products — SafeNet KeySecure supports a hardware root of trust using SafeNet Luna Hardware Security Modules (HSMs).

Highlighted capabilities

- **Heterogeneous Key Management.**
  Manage keys for a variety of encryption products including tokenization, and applications through SafeNet Data Protection Connectors, as well as self-encrypting drives, tape archives, Storage Area Networks, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.
- **Multiple Key Types.**
  Centrally manage Symmetric and Asymmetric Keys, secret data, and X.509 certificates along with associated policies.
- **Full Lifecycle Key Support and Automated Operations.**
  Simplify the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution, deactivation and deletion. Automated, policy driven operations simplify key expiry and rotation tasks.
- **Centralized Administration of Granular Access, Authorization Controls and Separation of Duties.**
  Unify key management operations across multiple encryption deployments and products, while ensuring administrators are restricted roles defined for their scope of responsibilities, from a centralized management console. Also, SafeNet KeySecure can utilize existing LDAP or AD directories to map administrative and key access for application and end users.
- **High-Availability and Intelligent Key Sharing.**
  Deploy in flexible, high-availability configurations within an operations center and across geographically dispersed centers or service provider environments using an active-active mode of clustering.
- **Auditing and Logging.**
  Detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading 3rd party SIEM tools.
- **Next-Generation Storage and Archive Solution.**
  Simplify secure storage and efficiently scale data centers while reducing costs and complexity, with SafeNet KeySecure and leading storage vendors such as NetApp, Dell, Nutanix, IBM, Hitachi, and HPE.

SafeNet KeySecure

SafeNet KeySecure offers customers a complete key management and data encryption platform providing the following advantages:

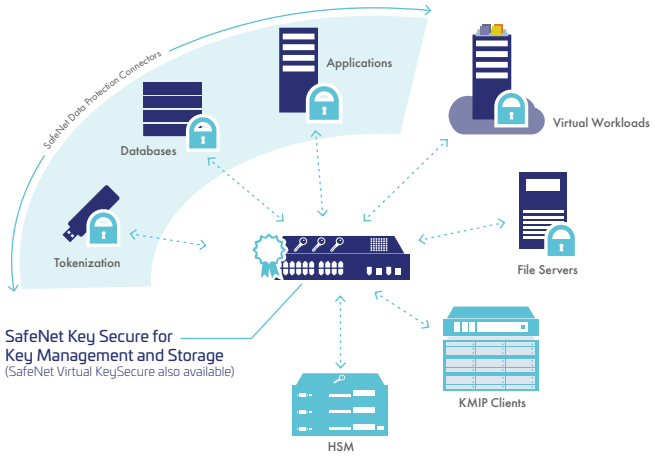
Single, centralized platform for managing cryptographic content (keys and related data) and applications capable of running on–premises, in the cloud or hybrid environments

SafeNet Crypto Pack – a simple licensing option that transforms your key management appliance into a server that includes support for the SafeNet Data Protection Connectors

SafeNet KeySecure benefits

- **Single, centralized platform** for managing cryptographic content (keys and related data) and applications
- **Use Case Expansion:** Transform your key management appliance into a server that includes support for the SafeNet Data Protection Connectors, SafeNet ProtectApp, SafeNet ProtectFile, SafeNet ProtectDB, and SafeNet Tokenization through the SafeNet Crypto Pack licensing option
- **Lower Administration Costs.** Lower the cost of key management and encryption with centralized administration and automated operations
- **Simplify Compliance.** Efficiently audit key management practices, save staff time, and simplify attainment of compliance mandates with efficient, centralized auditing of key management practices such as FIPS 140-2, PCI-DSS, HIPAA, GDPR
- **Lower Total Cost of Ownership.** Leverage a continuously growing list of 3rd party technologies leveraging Thales's Encryption Connector family of products and the OASIS KMIP standard
- **Risk Mitigation with Maximum Key Security.** Tamper-proof hardware options supporting a hardware root of trust with SafeNet Luna HSM
- **Turn Key Encryption.** In addition to its key management capabilities, the SafeNet KeySecure appliance offers customers the ability to perform high speed encryption/decryption operations as part of its capabilities. This allows customers to centralize encryption and crypto management operations regardless of its location

Safenet data protection connectors



Supported technologies (all models):

API Support

- Java, C/C++, .NET, XML open interface, KMIP standard

Network Management

- SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs & syslog, automatic log rotation, secured encrypted and integrity checked backups and upgrades, extensive statistics

Appliance Administration

- Secure Web-based GUI, Command Line Interface

Authentication

- LDAP and Active Directory

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

Looking for a virtual appliance?

Learn more about SafeNet Virtual KeySecure, which can be hosted on popular public and private cloud environments.

SafeNet KeySecure model comparison

SafeNet KeySecure			
	k460	**k450**	**k250**
Max keys	1,000,000	1,000,000	25,000
Max concurrent clients per cluster	1,000	1,000	100
Redundant HDs & PSU	Yes	Yes	No
FIPS 140-2 Support*	Level 3	Level 1	Level 1
SafeNet Data Protection Connectors**	Optional	Optional	Optional
RAM Required	8 GB Available	8 GB Available	1 GB RAM
Thales Third-party Integration Support	**Content Management:** Alfresco Open ECM, Open Text (EMC), InfoArchive Stealth Content Store, ServiceNow **Mainframe Encryption:** PKware **Big Data:** Dataguise, DataStax, Hadoop, MongoDB, MariaDB, SAP HANA, Cassandra, Couchbase, Hortonworks, CloudEra **Analytics**: IBM Qradar, HPE ArcSight, Splunk, RSA Security Analytics, Above Security **Application Servers:** IBM WebSphere, Oracle Weblogic, Microsoft IIS, Apache Tomcat, Red Hat JBoss **Backup Solutions:** Commvault Simpana, Symantec NetBackup (via NetApp) **Cloud Storage:** Nutanix, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive, NetApp Cloud ONTAP, NetApp AltaVault, IBM ICDES, Panzura Storage Controller **Cloud Access Security Brokers:** CipherCloud, SkyHigh Networks, Perspecsys (Blue Coat), Hitachi Sepaton VTL, CSC ServiceMesh, Netskope Active Encryption, Vaultive Cloud Data Protection Platform **Databases**: MS SQL Server (EKM), Oracle (TDE), IBM DB2, Oracle MySQL, Oracle Database, Teradata **File and Disk Encryption:** PKware, IBM, Dell, AWS, Microsoft, LUKS, ViaSat **Identity Management:** Centrify Privilege Service, Lieberman Software **Key Managers:** Hadoop KMS, CloudEra Navigator Key Trustee Server **Physical Storage:** NetApp NSE, Dell Compellent (SC and XC), HPE MSL/ESL Tape Libraries, HPE 3Par StoreServ, HPE XP7, Hitachi, SP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Series(i6000, i500 & i40/80),Viasat, Brocade FS8-18, Huawei Oceanstor, Tintri VMStore, Cisco UCS, SpringPath HyperFlex, NexentaStor 4.5		

* The SafeNet KeySecure k460 appliance supports a hardware root of trust using the SafeNet Luna HSM K6 card as part of its chassis.

** Remote encryption within the SafeNet KeySecure appliance using the connectors (SafeNet ProtectApp, SafeNet ProtectDB, and SafeNet Tokenization) requires the purchase of SafeNet Crytpo Pack. Local encryption, SafeNet ProtectV and SafeNet ProtectFile do NOT require SafeNet Crypto Pack feature activation.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • 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 – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com