Next Generation KeySecure

Overview

The Next Generation KeySecure™platform offers the industry leading enterprise key management solution enabling organizations to centrally manage their keys, protect data, and meet compliance requirements at a cost effective price-point. New Next Generation (NG) KeySecure models are available in multiple virtual and physical form-factors.

Your sensitive data is always protected from exposure and compromise, regardless of its location, be it stored in a database, file server, application, traditional or virtualized data center, or in private/public cloud environments.

Next Generation KeySecure Benefits

Host Anywhere:

- **Additional hosting options:** Virtual KeySecure images are provided for VMware, AWS, Microsoft Azure, OpenStack, Microsoft Hyper-V and Google Cloud Enterprise, with more public/private clouds coming soon.

Standards Compliance:

- **Built-in Hardware Security Module (HSM):** shipped with the k570 physical appliance, which provides cryptographic acceleration and a high assurance FIPS Certified root of trust.
- **Expanded HSM Integration:** Virtual KeySecure continues to offer integration with the Luna HSM portfolio, and also supports Data Protection on Demand (DPoD), AWS HSM and Azure Dedicated HSM. It helps secure backups with HSM binding.

Interoperability:

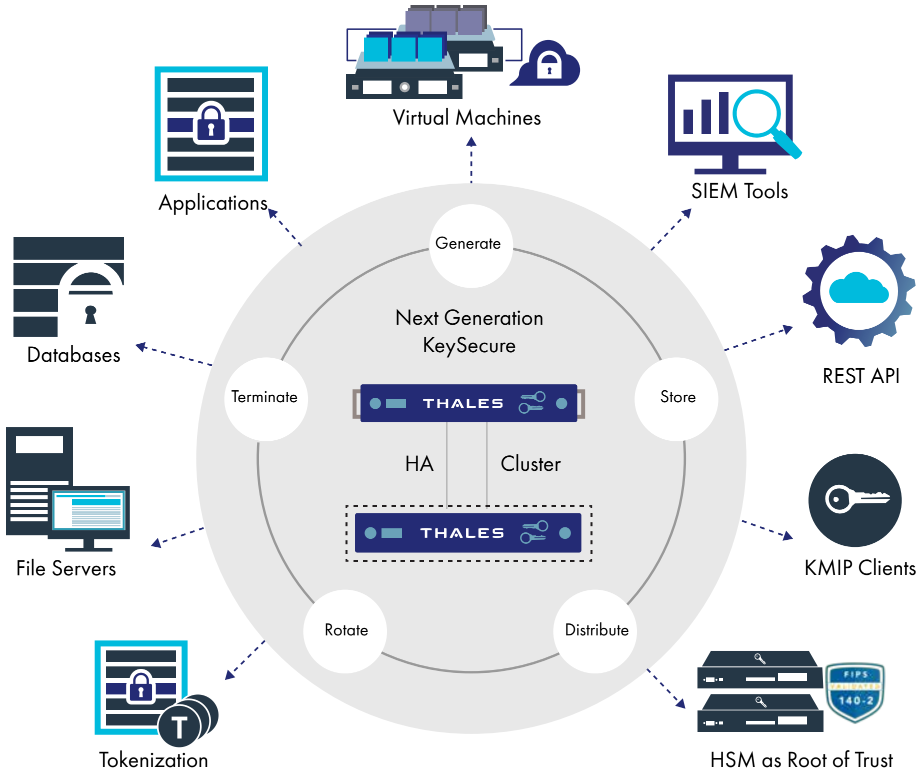
- **REST APIs:** available for developers to automate key management capabilities using DevOps tools such as, Ansible/Puppet/Chef. Combined with KMIP, PKCS#11, and other APIs, it supports standards based integration with a diverse range of third-party products (including BYOK for Public Cloud).
- **Broad spectrum of use-cases:** supported by the Thales data protection portfolio, with seamless migration for existing KeySecure customers.

Flexibility:

- **Adaptable HA Clustering:** Ability to pair a physical appliance with a virtual appliance for high availability configurations to lower cost and make it easy for lift and shift cloud migrations. Configurations can optionally include HSM as root of trust.
- **Subscription-based offerings:** that are better suited for operating expenditure (op-ex) models, versus capital expenditure models (standard hardware purchases) that require upfront payment.

Centralized Key Management:

- **Simplified Management Console:** GUI provides a clean, simple, user-friendly experience for commonly used functions like key management, user groups and permissions, and audit log review.
- **Consolidated Key security policies:** across multiple, disparate encryption systems, protecting current investments.
- **Centralized, efficient auditing:** of key management and licensing of the Data Protection Portfolio offers simplified compliance for cloud environments and decreases the amount of time spent on compliance mandates.



Highlighted Capabilities

- **Full Lifecycle Key Support and Automated Operations:** Simplifies management of encryption keys across the entire lifecycle, including secure key generation, storage and backup, and key distribution, deactivation and deletion. NG KeySecure makes automated, policy-driven operations easy for tasks such as key expiry and key rotation.
- **Centralized Administration of Granular Access, Authorization Controls, and Separation of Duties:** Management console unifies key management operations across multiple encryption deployments and products while ensuring that administrator roles are properly defined. Use existing LDAP or AD directories to map administrative and key access for application and end users.
- **High-Availability and Intelligent Key Sharing:** Deploys in flexible, high-availability configurations across geographically dispersed centers or service provider environments.
- **Auditing and Logging:** includes tracking of all key state changes, administrator access and policy changes in multiple syslog formats (RFC-5424, CEF, LEEF) for easier integration with SIEM tools. Audit trails are securely stored and signed for non-repudiation. In addition, customers can use SNMP to monitor appliance issues.
- **Heterogeneous Key Management:** Manage keys for a variety of encryption products including tokenization, and applications through Thales data protection connectors as well as a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard, REST or NAE XML.
- **Multiple Key Types:** Centrally manage symmetric and asymmetric key types as well as secret data and certificates (along with associated policies).

NG KeySecure Virtual Appliances:

	k470v	k170v
Max keys	1,000,000	25,000
Max concurrent clients per cluster	1,000	100
FIPS 140-2 Support	FIPS Compliant to level 1 Additional: Level 3 support with External HSM as Root of Trust	
Thales Data Protection Portfolio	Supported	Supported
System Requirements*	HD: 200GB or more RAM: 16 GB or more NICs: 2 or more CPU: 4 or more	HD: 100GB RAM: 4-8 GBB NICS: 1 -2 CPU: 2 or more
APIs Supported	REST KMIP PKCS#11 JCE,.NET,MSCAPI, MS CNG, NAE-XML	
Use Case**	High transaction environments	Low-Medium transaction environments

* These minimum system requirements are for a system with light to moderate load. For applications that heavily load the system, additional memory and CPU allocation are required.

* High transaction environment are scenarios where customer requires high transaction per second (TPS) throughput for the encryption and decryption of data. Low-Medium transaction use cases would be ones where the key is infrequently accessed (such as KMIP for storage integrations)

NG KeySecure Physical Appliances:

	K570	K470
Max keys	1,000,000	1,000,000
Max concurrent clients per cluster	1,000	1,000
FIPS 140-2 Support*	Level 2 compatible chassis with Level 3 Certified HSM Card in Appliance	Level 2 compatible chassis
Thales Data Protection Connectors	Supported	
API's Supported	REST KMIP PKCS#11 JCE,.NET,MSCAPI, MS CNG, NAE-XML	
NIC Options	4x1GB 2x10GB/2x1GB NIC Bonding Supported	

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.

Learn More

Thales Key Management solutions

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) Ltd
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

> cpl.thalesgroup.com <