

SafeNet KeySecure™

PRODUCT BRIEF

Enterprise Key Management

- Consolidated key security policies across multiple disparate encryption systems
- Automated, centralized key generation, storage, rotation, and expiration policies
- Separation of duties through individual or group level authorization, and defined key validity timeframes
- Verifiable audit trail for all key management actions to address compliance requirements
- Supports KMIP and standard management protocols from legacy devices
- Ensure encrypted data is continuously secure and available with an easy to use, self-contained, hardened hardware solution
- Centralized and consistent enterprise-wide key management across physical and virtual datacenters, disaster recovery sites and cloud infrastructures
- Next-generation key management solution for NetApp DataFort Encryption Appliance, NetApp Storage Encryption (NSE) and NetApp Lifetime Key Manager (LKM)

Simplify key management while maximizing key security for physical, virtual and cloud

Today's enterprise consists of fragmented encryption solutions that have proliferated through internal projects and compliance mandates, across multiple tiers and multiple vendor platforms, from physical and virtual data centers to disaster recovery sites and cloud leaving organizations in a management and operational quandary. Implementing encryption is fundamental for solving compliance mandates, addressing security policies to avoid audit failures, and protecting intellectual property; however, as the number of encryption solutions increase, the number of encryption keys and associated key stores grow. Security teams struggle to contend with the administrative effort of managing not only encryption deployments but also the associated key lifecycle operations. A centralized enterprise key management solution is crucial for managing the keys protecting the data.

SafeNet KeySecure™ offers a robust enterprise key management solution with the ability to consolidate and centrally manage encryption keys from multiple, disparate encryption platforms. KeySecure™ simplifies the operational challenges of managing encryption keys—ensuring keys are secure and information is always available to authorized users. As the use of encryption proliferates throughout an organization, security teams must be able to easily scale their management of encryption keys, including key generation, key import and export, key rotation, and much more. Administrators can simultaneously manage multiple appliances and associated keys, including storage devices such as self-encrypted disks and tape drives, storage encryption platforms, virtual storage, virtual machine instances, encrypted applications, files, hard disks, and more. With SafeNet KeySecure™, security teams gain the critical key management capabilities they need to secure physical, virtual, and cloud-based environments while enforcing security policies surrounding access and use.

Heterogeneous Key Management

Multiple encryption solutions lead to decentralized key management strategies, increasing administration, management, and maintenance costs. SafeNet KeySecure™ centralizes the management of cryptographic objects into a single, central and secure platform. KeySecure™ securely manages a variety of encryption and data protection solutions, including storage and archive encryption systems, SAN switches using encryption, applications, hardware security modules (HSMs) and virtual machine instances in the data center or the cloud. By conforming to the OASIS Key Management Interoperability Protocol (KMIP) standard, KeySecure™ can also consume and manage keys from KMIP-compliant solutions in addition to proprietary encryption protocols from existing or legacy systems. KeySecure centrally manages symmetric and asymmetric encryption keys and policies, secret data for password management and x.509 encryption certificates. KeySecure™ also offers a set of APIs to manage keys for home-grown encryption implementations.

Key Features

KeySecure Security

- NIST FIPS 140-2 Level 3 for SafeNet LUNA® PCI-e Cryptographic Module embedded encryption card

Virtual KeySecure Security

- Hardened Operating System
- VMware ESXi 4 and ESXi5 platform or hypervisor

Key Management

Asymmetric

- 1024, 2048, 3072, 4096

Symmetric

- 128, 192, 256

Secret Data

- Hash value of passwords

X.509 Certificates

Key Management Protocol

OASIS KMIP (Key Management Interoperability Protocol) 1.0 Specification compliant

- NIST 800-57 Key Lifecycle support
- Symmetric Key, Asymmetric Key, Opaque, Secret Data, Template
- Operations: Create, Register, Get, GetAttribute, GetAttributeList, Locate, Query, Add/Delete/Modify Attributes

Role-based Management Control

- Multiple restricted roles can be defined for each administrator
- Automated, self-contained key management
- Multi-credential administrative authorization for sensitive security operations

Key Availability and Capacity

- Secure key replication to multiple appliances
- Intelligent key sharing via key sharing groups

High Availability and Redundancy

- Active-Active mode of clustering
- Multiple geographies
- Hierarchical clustering

Supported Technologies

API Support

- KMIP, PKCS #11, JCE, MSCAPI, and .NET

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

System Administration

- Secure Web-based GUI, Secure Shell (SSH), and console

Supported Directory Services

- LDAP and Active Directory services

Centralized Monitoring and Management of Encryption Keys

Disparate encryption solutions with fragmented key management lead to key management silos, each with their own enforcement policy. KeySecure™ simplifies key management, making it efficient for security teams to consolidate data security over time and across the enterprise. With KeySecure™, administrators can create hierarchical key-sharing groups that enable fast, efficient key management across multiple organizations—while ensuring relevant policies for different groups are consistently enforced. Centralized key management reduces audit-scope for compliance, and ensures stronger data use and tracking control for operational efficiency. KeySecure™ provides a secure repository for all sensitive crypto objects, including symmetric and asymmetric keys and certificates.

Ensure Root of Trust

Compliance mandates, and the move to distributed and virtual/cloud-based data centers, increase the need for enterprise key management. With this move comes the concern of maintaining control over data on systems that may be shared and managed by other organizations. KeySecure™, the anchor of trust, offers a tamper-proof hardware appliance based on a hardened platform or a virtual security appliance encrypted with a hardened OS. Data may reside locally, virtually or in the cloud but the keys and defined user access controls securely reside within KeySecure™. Organizations control user access to data, while providers control the maintenance of the appliances without gaining access to the data that resides on those systems.

Granular Key Administration

KeySecure™ protects data with unique keys based on its informational value and on internal business policies. Encryption keys are tied to users based on defined access and usage policies. Even in instances of multi-tenant environments or on devices where information is stored or shared between groups, departments, partners, and customers, our granular key administration allows for the co-mingling of data without compromising or exposing data. KeySecure™ enables granular authorization controls based on user key permissions. Existing administrator, security and user access controls can be automatically retrieved from existing LDAP/Active Directory services and further defined within the KeySecure™ Administration console to provide an additional layer of access management.

KeySecure Benefits

Centralized Key Administration. A single key management console provides a centralized and comprehensive view for managing and maintaining a wide assortment of encryption solutions and scales easily to accommodate new encryption solutions. KeySecure™ allows administrators to consolidate and centrally manage encryption keys, passwords, and certificates from a single location, removing the challenge of ongoing maintenance, management, and auditability associated with disparate encryption solutions. Consolidating key management allows administrators to monitor all encryption key activities for tape and disk-based storage platforms, SAN switches, applications, hardware security modules (HSMs), virtual machine instances and more.

Deployment Options

KeySecure k460

- Up to 1 million symmetric & asymmetric keys, secret data and certificates stored per cluster
- Up to 1,000 concurrent clients
- Intel Xeon E5620 2.4Ghz, 12M Cache, Turbo, HT, 1066MHz Max Mem processor
- Four (4) 10/100/1000 Mbps Ethernet ports
- Two 500GB 7.2K RPM SATA 2.5" Hot-Plug Hard Drives
- 1U, rack mountable (H: 1.7"; W: 19"; D: 30")
- Two 502W Energy Smart Hot-Plug power supplies
- Embedded SafeNet LUNA® PCI-e Cryptographic Module

Supported Appliances

Hardware Security Modules (HSM)

- SafeNet LUNA SA
- SafeNet LUNA PCI

Storage Encryption Appliance

- SafeNet StorageSecure
- NetApp E-Series DataFort
- Hitachi Virtual Storage Platform

FDE Storage

- NetApp NSE

SAN Switches

- Brocade Encryption Switch
- Brocade FS8-18 Encryption Blade

Tape Libraries

- HP ESL G3
- Quantum Scalar Series i6000, i500 and i40/i80

Application Encryption

- SafeNet ProtectApp, iCAPI/KMIP, JCE/KMIP

Cloud Encryption/Virtual Instances

- SafeNet ProtectV

KMIP-compliant clients

KeySecure k150

- Up to 25,000 symmetric & asymmetric keys, secret data and certificates stored per cluster
- Up to 100 concurrent clients
- VIA C3 800MHz processor
- One (1) 10/100 Mbps Ethernet port
- 250W, 100 - 240 VAC, auto-ranging, 50-60 Hz, 5 - 3A power supply
- 1U, rack mountable (H: 1.7"; W: 19"; D: 13")

Supported Appliances

Tape Libraries

- HP ESL G3
- Quantum Scalar Series i6000, i500 and i40/i80

Application Encryption

- SafeNet ProtectApp, iCAPI/KMIP, JCE/KMIP

Cloud Encryption/Virtual Instances

- SafeNet ProtectV

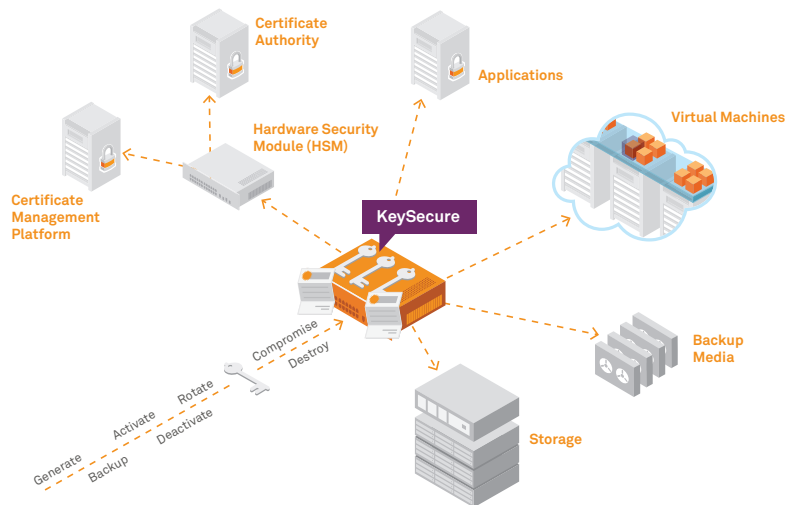
KMIP-compliant clients

Virtual KeySecure k150v

- Up to 25,000 symmetric & asymmetric keys, secret data and certificates stored per cluster
- Up to 100 concurrent clients

Supported Appliances

- Cloud Encryption/Virtual Instances
- SafeNet ProtectV



X.509 Certificate Management. KeySecure™ supports a variety of cryptographic objects from symmetric and asymmetric keys, secret data for password management and X.509 certificates. By adding management of X.509 certificates, KeySecure™ provides a single, centralized and highly secure key management repository for multiple cryptographic objects. Certificate management capabilities enable administrators to proactively manage and monitor certificates and their attributes - such as issuer, validity dates, subject and public key information - while maintaining a single management point for compliance and governance.

KMIP Compliant. SafeNet, one of the primary vendors driving the Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP), has built KeySecure™ in accordance to the KMIP standard. Point encryption solutions have created fragmented key stores, forcing administrators to manage and maintain keys for multiple encryption types and multiple encryption appliances. KeySecure™, with its conformance to the OASIS KMIP specification, enables administrators to manage cryptographic modules and storage devices from different vendors that are using different management consoles within a single centralized management system.

Maximize Security. Based on a hardened security appliance, KeySecure™ safeguards keys against theft, tampering, and unexpected system failures. KeySecure™ centralizes all key management activities, including key signing, role-based administration, quorum control, and the backup and distribution of encryption keys across the enterprise. Keys and associated attributes are signed to protect their integrity for their lifetime. For sensitive security operations, KeySecure™ allows you to stipulate multiple credential authorization from more than one administrator. The administrators share credentials for a defined period of time required to confirm the operation.

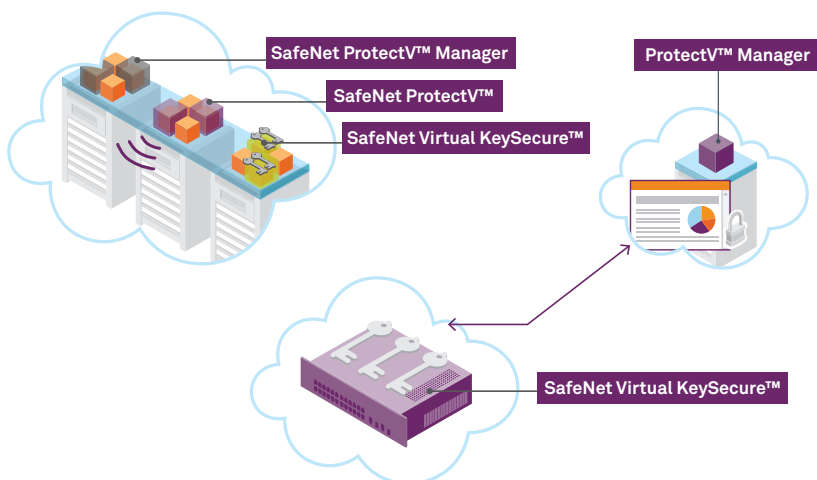
Separation of Duties. KeySecure™ supports granular authorization, enabling constraints to be placed on specific key permissions. This makes KeySecure™ perfect for protecting against insider threats through segmented key ownership based on individuals or group owners. KeySecure integrates with user directories such as LDAP, Microsoft AD, and other directory services to incorporate existing user access controls.

Auditing, Logging, and Alerting. KeySecure™ has built-in auditing, logging, and alerting for facilitating compliance mandates. All keys, certificates and passwords are securely managed, key ownership is clearly defined and key lifecycle management and modifications are recorded and securely stored providing a non-repudiative audit trail of key state changes. Administrators and security personnel are informed if attempts to breach protected keys have occurred.

Key Destruction. Compliance initiatives require organizations to implement key disposal policies when data is retired or replaced, and when the integrity of the key has been weakened or compromised. Storing encryption keys centrally within KeySecure™ allows administrators to easily manage keys without accessing individual hardware or software appliances. By retiring the key, KeySecure™ ensures that stored sensitive data is rendered unreadable in the event the appliance needs to be repurposed, the data needs to be destroyed, or if the key has been compromised.

Resiliency and Availability. KeySecure™ clustering enables multiple KeySecure appliances to share configuration settings in an active-active mode. Configuration changes are replicated instantly to all the members within the same cluster. Immediate configuration sharing between all of the nodes within the cluster improves the failover capabilities and fault resiliency drastically in geographically disbursed large data center deployments. Information is shared between all the nodes over a secure communication channel so that sensitive data remains protected while in transit. Replication is supported by an automatic re-try, SNMP failure notification, and a manual synchronization to mitigate network-related issues in a large deployment across the globe.

Virtualization/Cloud Ready. By virtualizing key management organizations are able to take advantage of virtualization and the cloud while ensuring consistent enterprise-wide security and operational efficiency. Cloud data can be exposed to cloud administrators, co-resident lawful surrender, or easily copied and destroyed if the data is not properly encrypted and keys securely stored. Virtual KeySecure™ is a virtual security appliance, hardened and secured to protect encryption keys. With elastic pay-as-you-go scaling and low TCO for virtualized and cloud infrastructures, Virtual KeySecure™ images are easily provisioned to departments, customers, and partners enabling security thought out the supply chain. Regardless of the location of data, KeySecure™ is only accessible to authorized administrators and users. KeySecure™ is highly suited for dense virtual or cloud environments with established virtual infrastructures or to customers migrating to a virtual environment. Cloud administrators are able to manage and maintain servers without accessing the data or risking data security.



Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: www.safenet-inc.com/connected

©2013 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB (EN)-02.20.13