SafeNet KeySecure

PRODUCT BRIEF

Enterprise Key Lifecycle 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

- Trusted vendor with a strong security and encryption ancestry

- Next-generation key management solution for NetApp DataFort and LKM

Simplify key management while maximizing key security from electronic and physical attacks

Today's enterprise consists of fragmented encryption solutions that have proliferated through internal projects and compliance mandates, across multiple tiers and multiple vendor platforms, 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. The data is only as secure as the system managing the keys that protect it. A centralized enterprise key lifecycle management solution is crucial for managing the keys protecting the data.

SafeNet KeySecure offers a robust enterprise key lifecycle 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 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 instances, encrypted applications, files, hard disks, databases, 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.

Simplifies Heterogeneous Key Management

Multiple encryption solutions lead to decentralized key management strategies, increasing administration, management, and maintenance costs. SafeNet's KeySecure manages a variety of encryption and data protection solutions, including applications, databases, storage devices, SAN switches, tape libraries, network and endpoint devices, and protection of virtual instances in the cloud. By conforming to the OASIS KMIP standard, KeySecure can 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, key policies, servers, hardware security modules, and data access. KeySecure also offers a set of APIs to manage keys for home-grown encryption implementations.

Key Features

Security
- NIST FIPS 140-2 Level 3 for SafeNet LUNA® PCI-e Cryptographic Module embedded encryption card (validation in process)

Cryptography:
- AES, 3DES, DES, RSA (signatures and encryption), RC4, HMAC SHA-I – SHA512, SEED encryption
  - Asymmetric key sizes
    - 1024, 2048, 3072, 4096
  - Symmetric key sizes
    - 128, 192, 256

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, CreateKeyPair, 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
- iCAPI, 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 Key Management
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. 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 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, is a tamper-proof hardware appliance based on a hardened platform. Data may reside off premise but the keys and the defined user access controls reside locally with KeySecure, allowing organizations to secure all data whether it resides locally, virtually, or in the cloud. 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 allows administrators to manage encryption keys and their lifecycle for disparate encryption solutions in a central location. Consolidating key management allows administrators to monitor all encryption key activities for tape and disk-based storage platforms, SAN switches, databases, applications, and more. Furthermore, KeySecure streamlines the secure backup and recovery of sensitive data.

- Secure, centralized key management
- Standards-based via KMIP
- Data-centric policy management
- Highly available and scalable
- Identity and access management
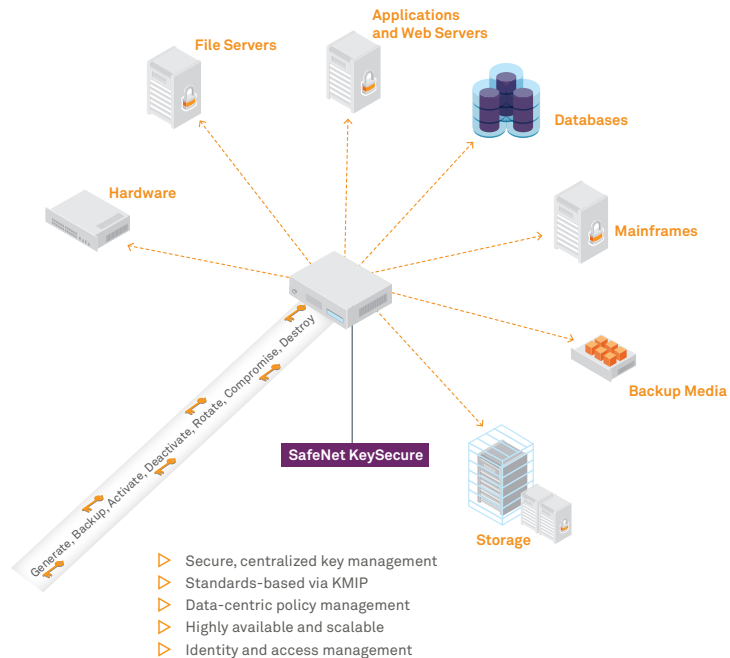
KMIP Compliant. SafeNet, one of the primary vendors driving the Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP), has built KeySecure in accordance to the KMIP standard. Point encryption solutions have created fragmented key 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 user operations based 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 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.

Ease of Deployment. KeySecure is a hardened, self-contained key management appliance that easily assimilates into your environment. There are no servers to set up or software to install and maintain, reducing your operating costs, and freeing security and IT personnel. KeySecure is ready to store and manage keys.   As your environment grows and evolves, KeySecure appliances can be easily added as needed. Keys are automatically replicated among nodes of the cluster.

Ease of Integration. KeySecure offers open APIs that provide easy integration with virtually any off-the-shelf encryption product, including database encryption, laptop and device encryption, file and storage level encryption, and more. SafeNet supports a wide range of open cryptographic standard interfaces, including PKCS #11, JCE,MSCAPI, and .NET. KeySecure is an OASIS KMIP-compatible key management server. KMIP-compatible cryptographic clients can communicate with KeySecure for their key management needs. Customers and partners can take advantage of SafeNet's XML interface to develop their own custom software utilizing the enterprise key management functionality of KeySecure.

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.

Cloud Ready. 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. KeySecure can reside within the local data center or public cloud, and can easily protect cloud encryption solutions. Regardless of its location, KeySecure and the associated data is only accessible to authorized administrators and users. KeySecure is highly scalable for large implementations across cloud zones and cloud providers. Cloud administrators are able to manage and maintain servers without accessing the data or risking data security.