PRODUCT BRIEF

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 Gemalto 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 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 Gemalto’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 KeySecure Model Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>k460</th>
<th>k450</th>
<th>k250</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max keys</td>
<td>1,000,000</td>
<td>1,000,000</td>
<td>25,000</td>
</tr>
<tr>
<td>Max concurrent clients per cluster</td>
<td>1,000</td>
<td>1,000</td>
<td>100</td>
</tr>
<tr>
<td>Redundant HDs &amp; PSU</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FIPS 140-2 Support*</td>
<td>Level 3</td>
<td>Level 1</td>
<td>Level 1</td>
</tr>
<tr>
<td>SafeNet Data Protection Connectors**</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>RAM Required</td>
<td>8 GB Available</td>
<td>8 GB Available</td>
<td>1 GB RAM</td>
</tr>
</tbody>
</table>

** Gemalto Third-party Integration Support**

- Content Management: Alfresco Open ECM, Open Text [EMC], InfoArchive Stealth Content Store, ServiceNow
- Mainframe Encryption: PKware
- Big Data: Datafuse, DataStax, Hadoop, MongoDB, MariaDB, SAP HANA, Cassandra, Couchbase, Hortonworks, CloudEra
- Analytics: IBM Gradir, 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 ICD5, Panzura Storage Controller
- Cloud Access Security Brokers: CipherCloud, SkyHigh Networks, Perspectiva [Blue Coat], Hitachi Sepaton
- VTL, CSC ServiceMesh, Netskope Active Encryption, Vaultrue Cloud Data Protection Platform
- Databases: MS SQL Server (EKMS), 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 XP9, Hitachi, SP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Series[6000, i500 & i40/80], Viasat, Brocade FSB-18, Huawei Oceanstor, Tivoli 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 uses the connectors (SafeNet ProtectApp, SafeNet ProtectDB, and SafeNet Tokenization) requires the purchase of SafeNet Crypto Pack. Local encryption, SafeNet ProtectV and SafeNet ProtectFile do NOT require SafeNet Crypto Pack feature activation.

Looking for a virtual appliance? Learn more about SafeNet Virtual KeySecure, which can be hosted on popular public and private cloud environments.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us/
Follow Us: blog.gemalto.com/security

©Gemalto 2017. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. P. B., EN J. Sep 28, 2017 - Design FR