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 and hardened virtual 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 Network Hardware Security Modules (HSM) or the Amazon CloudHSM service.

Highlighted Capabilities

- **Heterogeneous Key Management.** Manage keys for a variety of encryption products including tokenization, and applications through SafeNet Crypto Pack, as well as self-decrypting 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 encryption 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.
- **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.
- **Security and Compliance for Cloud Environments.** Take advantage of the lower costs of virtualized and cloud environments with flexible deployment options and appliance models covering physical, and virtual environments (VMware and AWS Marketplace).
- **Risk Mitigation with Maximum Key Security.** Tamper-proof hardware options and hardened virtual appliance supporting a hardware root of trust with SafeNet’s Network HSM or using Amazon’s CloudHSM service.
- **TurnKey Encryption.** In addition to its key management capabilities, the 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

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 Gemalto encryption connectors SafeNet ProtectApp, SafeNet ProtectFile, SafeNet ProtectDB, and SafeNet Tokenization.
Available Solutions:

SafeNet KeySecure k460 & k450
- Capacity for large number of keys and encryption transactions

SafeNet KeySecure k250
- Designed for small / medium businesses
- FIPS 140-2 Level 1

SafeNet Virtual KeySecure k150v
- FIPS 140-2 Level 1 validation
- Virtual security deployed on VMware (ESXi 4 and ESXi 5) or AWS Marketplace
- Hardened OS
- Hardware root of trust using SafeNet Network HSM or Amazon’s CloudHSM Service for master key

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

---

SafeNet KeySecure Model Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>k460</th>
<th>k450</th>
<th>k250</th>
<th>k150v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max keys</td>
<td>1,000,000</td>
<td>1,000,000</td>
<td>25,000</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>
<td>100</td>
</tr>
<tr>
<td>Redundant HDs &amp; PSU</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>FIPS 140-2 Support</td>
<td>Level 3</td>
<td>Level 1</td>
<td>Level 1</td>
<td>Level 1</td>
</tr>
<tr>
<td>HSM Integration*</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SafeNet Crypto Pack**</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>CPU</td>
<td>1 CPU Required</td>
<td>1 CPU Required</td>
<td>1 CPU Required</td>
<td>1 CPU Required</td>
</tr>
<tr>
<td>RAM 1024 MB Ram Required</td>
<td>1024 MB Ram Required</td>
<td>1024 MB Ram Required</td>
<td>1024 MB Ram Required</td>
<td>1024 MB Ram Required</td>
</tr>
<tr>
<td>Disk Space Required for Install</td>
<td>150G</td>
<td>150G</td>
<td>150G</td>
<td>150G</td>
</tr>
</tbody>
</table>

Gemalto third-party integration Support

- 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, Panzura Storage Controller
- Cloud Access Security Brokers: CipherCloud, SkyHigh Networks, Perspectus (Blue Coat), Hitachi Sepaton VTL, CSC ServiceMesh, Netskope
- Databases: Microsoft SQL Server, Oracle (DBE), IBM DB2, Oracle MySQL, Oracle Database, Teradata
- File and Disk Encryption: PKware, MongoDB
- Identity Management: Centrify Privilege Service
- 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 VSP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Seriesi6000, i500 & i40/80, Viasat, Brocade F58-18

About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of SafeNet Identity and Data Protection solutions enables enterprises, financial institutions and governments to protect data, digital identities, payments and transactions—from the edge to the core. Our solutions take a data-centric approach to security with innovative encryption methods, best-in-class crypto management, and strong authentication and identity management to help customers protect what matters, where it matters.

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

Follow Us: data-protection.safenet-inc.com

©Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. SB (EN)-May062016 - Design: FR