PRODUCT BRIEF

SafeNet Virtual KeySecure

Overview
SafeNet Virtual KeySecure™ is a hardened virtual security appliance that provides organizations with a more operation—and expense friendly alternative to using a hardware appliance for secure key management and meeting security and compliance requirements. By using a virtual key manager instead of a hardware appliance, organizations can scale key management in private or public cloud infrastructures, and eliminate the cost for additional rack space. SafeNet Virtual KeySecure allows organizations to utilize a secure virtual appliance to manage keys as well as data encryption, and enforce access control across cloud infrastructures. It also ensures that organizations maintain ownership of their encryption keys at all times by hardening the appliance OS and encrypting the entire virtual appliance for enhanced key security and protection against snapshot attacks.

SafeNet Virtual KeySecure, the New Generation
Gemalto’s latest SafeNet Virtual KeySecure product is the k170v model, which is built on prevailing cloud-based technologies and provides a cloud friendly, key management solution for your organization.

With a REST interface and microservices based architecture, the k170v has been built to easily deploy and scale within your environment. Using the new REST API Playground, developers can explore the new set of key management and administrative endpoints.

Organizations can lower costs and scale key management with a virtual appliance that is quickly deployed for high-availability in various public cloud infrastructures such as Oracle, AWS and Microsoft Azure, or on-premise using Oracle VM VirtualBox VMware vSphere, and Openstack.

Combat Risk and Get Affordable Security
As companies migrate to virtual data centers and cloud environments, sensitive data is likely to reside outside the physical walls of the enterprise, making secure data management a challenge. With regulations such as PCI DSS, HIPAA/HITECH, GDPR, GLBA, and SOX, combined with the high cost of data breaches, the pressure to protect this sensitive data has never been greater.

SafeNet Virtual KeySecure provides customers with a virtual appliance that manages and securely stores encryption keys for diverse encryption solutions, including the SafeNet Data Protection portfolio, traditional storage and hyperconvergence solutions, Big Data, KMIP compliant solutions, and many others. Gemalto is the only solutions provider that offers a virtual key management appliance integrated with a hardware root of trust (SafeNet Luna Hardware Security Modules (HSM) or Amazon CloudHSM) that can be employed in the public cloud.

SafeNet Virtual KeySecure Benefits

**Host Anywhere:**
- The k150v and k450v models can be rented from a service such as AWS marketplace, or hosted on any virtual environment such as Oracle VM Virtual Box, IBM Marketplace, AWS and others.
- **New!** The SafeNet Virtual KeySecure k170v model provides additional hosting options, and can run as a native virtual machine on VMware, AWS, Microsoft Azure, Oracle VM Virtual Box and OpenStack with more public/private clouds coming soon.

**Compatibility:**
- Compatibility with the OASIS Key Management Interoperability Protocol (KMIP) standard provides support for a large and growing list of encryption products.
- Support of the SafeNet Data Protection portfolio provides customers with a broad spectrum of use cases that can be supported.
- **Bring Your Own License (BYOL) for AWS Marketplace enables purchase directly from Gemalto (available for the k150v and k450v models).**

**Flexibility:**
- Subscription-based offerings that are better suited for operating expenditure (op-ex) models, versus capital expenditure models (standard hardware purchases) that require upfront payment.
- Flexible deployment options can easily scale to provide key management at remote facilities or in cloud infrastructures.
- A newly designed GUI for the k170v model provides a clean, simple, user-friendly experience for commonly used functions like key management, user groups and permissions, and audit log review.

**Centralized Key Management:**
- Key security policies can be consolidated across multiple, disparate encryption systems, protecting current investments.
- Centralized, efficient auditing of key management offers simplified compliance for cloud environments and decreases the amount of time spent on compliance mandates.

SafeNet Virtual KeySecure Use Cases
SafeNet Virtual KeySecure provides application data protection and centralized key management for Gemalto and third-party encryption products across stored and archived data, virtual workloads, and application data protection.
**Product Highlights:**

- 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. SafeNet Virtual 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.
- High-Availability and Intelligent Key Sharing. Deploys in flexible, high-availability configurations across geographically dispersed centers or service provider environments.
- Auditing and Logging. Centralized management includes 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.

**Virtual KeySecure Model Comparison**

<table>
<thead>
<tr>
<th>Features</th>
<th>k170v</th>
<th>k450v</th>
<th>k150v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Keys</td>
<td>25,000</td>
<td>1,000,000</td>
<td>25,000</td>
</tr>
<tr>
<td>Max concurrent Clients per Cluster</td>
<td>100</td>
<td>1,000</td>
<td>100</td>
</tr>
<tr>
<td>FIPS 140-2 Support</td>
<td>L3 w/ HSM integration</td>
<td>L3 w/ HSM integration</td>
<td>L3 w/ HSM integration</td>
</tr>
<tr>
<td>HSM Integration *</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports KMIP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CPU</td>
<td>2 CPU Required</td>
<td>12 CPU (Configurable)</td>
<td>1 CPU Required</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB RAM (Configurable)</td>
<td>8192 MB (Configurable)</td>
<td>1024 MB Ram Required</td>
</tr>
<tr>
<td>Network Adaptor</td>
<td>1 Allowed/Available</td>
<td>2 (Configurable)</td>
<td>1 Allowed / Available</td>
</tr>
<tr>
<td>Interface / Architecture</td>
<td>REST API</td>
<td>NAE-XML</td>
<td>NAE-XML</td>
</tr>
<tr>
<td></td>
<td>NAE-XML</td>
<td>KMIP</td>
<td>KMIP</td>
</tr>
<tr>
<td>Supported Cloud Environments</td>
<td>AWS, MS Azure, VMware vsphere, Oracle VM Virtual Box and OpenStack</td>
<td>Can be hosted on a virtual machine running VMware or rented from a service such as AWS Marketplace</td>
<td>Can be hosted on a virtual machine running VMware or rented from a service such as AWS Marketplace</td>
</tr>
<tr>
<td>Gemalto Third-party Integration Support</td>
<td>Content Management: Open Text (EMC Infoblox), Stealth Content Store, ServiceNow, VMcrypt</td>
<td>Mainframe Encryption: PKWARE</td>
<td></td>
</tr>
</tbody>
</table>

*Supports key storage in hardware security modules (HSMs) such as Amazon Web Services CloudHSM in a subscription-based AWS environment, and SafeNet Luna HSM, a hardware appliance option that is deployed on-premises in a range of models and configurations.

**Try it before you buy it.** [Click here](https://blog.gemalto.com/security) to enroll in Amazon Web Services 30-day free trial.

**Need an on-premise appliance?** Learn more about on-premises enterprise key management.

**Contact Us:** For all office locations and contact information, please visit [https://safenet.gemalto.com/contact-us/](https://safenet.gemalto.com/contact-us/)

**Follow Us:** [blog.gemalto.com/security](https://blog.gemalto.com/security)