Managing SafeNet Luna HSM with SafeNet KeySecure 6.1

SOLUTION BRIEF

KeySecure 6.1 and Luna HSM Features

Key Monitoring:
KeySecure allows tracking of all the keys stored in Luna HSM (as well as other key-vaults), logging and monitoring of key creation, deletion, and usage, including their exact location (in which HSMs they are located) and their metadata and attributes for easier management.

Remote Key Foundry:
Using KeySecure 6.1 and the KeySecure client for Luna HSM security administrators can ensure that cryptographic keys are created using single management system. This feature allows an administrator to remotely invoke the creation of a key in an HSM registered with KeySecure 6.1.

Simple, Straight Forward Setup and Configuration:
Managing encryption keys used by Luna HSM, through keys' life cycle is done in an easy and straight-forward manner using KeySecure.

As data security risks increase, and enterprises are confronted with a variety of regulations as well as their internal risk management requirements, the use of cryptography as a method for data protection is spreading. However, the manner in which data protection solutions have been deployed has led to "Encryption Silos" - fragmented security solutions, each with its own cryptographic key-vault and management system. As security needs have grown, organizations have implemented an increasing number of these dispersed encryption silos, making these solutions difficult and costly to manage and monitor.

Establishing effective key- and security-policy management is a critical component in such environments. A policy-based approach to key management provides the flexibility and scalability needed to support data protection requirements today and into the future. Centralized, policy-based key management ensures the secure administration of keys throughout their entire lifecycle, including generation, distribution, usage, storage, recovery, termination, and archival. This also improves business productivity and relieves over-burdened IT staff by converging these "security silos" into a unified centralized environment that is easier to control.

SafeNet KeySecure 6.1 offers an enterprise key lifecycle management platform with the ability to consolidate and centrally manage and monitor cryptographic keys from multiple, disparate platforms. Together with SafeNet Luna HSM, the combined solution simplifies the operational challenges of monitoring the use of cryptographic keys, which is needed as part of a complying with many info-security standards and for ensuring data-protection according to the highest security standards.

Centralized Key Management and Monitoring using SafeNet's KeySecure 6.1 and Luna HSM

KeySecure, SafeNet's key management platform, simplifies key management, enabling security teams to consolidate data-protection solutions over time and across the enterprise. KeySecure support for an industry standard key management protocol - Key Management Interoperability Protocol (KMIP) - enables organizations to use the solution to manage their security infrastructure, knowing that as their security needs and industry solutions evolve, KeySecure will continue to manage their keys effectively.

Luna HSM support for KMIP enables it to be managed by KeySecure 6.1, ensuring a centralized key-management and monitoring solution. The solution enables organizations to monitor their keys from a centralized location. Ensuring events as key-creation, encrypting and decrypting with managed keys and key-deletion are all documented and centrally tracked.

Centralized Administration of SafeNet HSMs with KeySecure
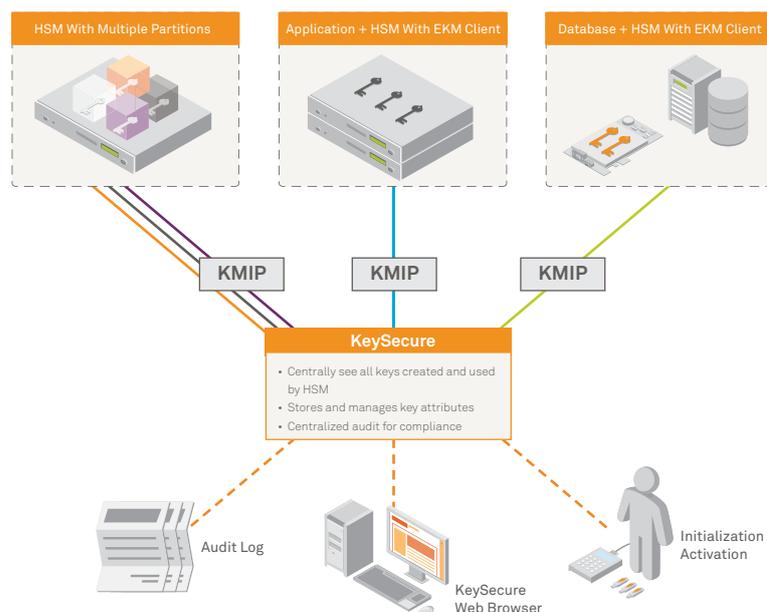
SafeNet Hardware Security Modules

As businesses transform and use sensitive data within their enterprise and in the cloud, it is imperative to ensure trusted ownership. SafeNet Hardware Security Modules (HSMs) provide reliable protection for transactions, identities, and applications by securing cryptographic keys and providing encryption, decryption, authentication, and digital signing services. SafeNet HSMs are ranked #1 in the market worldwide. They provide the highest-performing, most secure, and easiest-to-integrate application and transaction security solution for enterprise and government organizations. Robust and temper-resistant, SafeNet HSMs are FIPS and Common Criteria validated to ensure compliance with stringiest information security regulations.

With a broad range of HSM offerings and a full range of API support, SafeNet HSMs enable application developers to easily integrate security into custom applications. In partnership with leading application solution providers, SafeNet has produced HSMs that offer end-to-end protection for organizations, helping them achieve regulatory compliance, streamline business processes, reduce legal liabilities, and improve profitability.

SafeNet KeySecure

SafeNet KeySecure is an Enterprise Key Management (EKM) solution that enables a single, centralized solution for managing cryptographic keys and policies. As the use of encryption proliferates throughout the corporation, security teams must scale their management of encryption keys, including key generation, key import and export, key rotation, and much more. With KeySecure, administrators can simultaneously manage multiple, disparate encryption appliances and applications' associated keys through a single, centralized key management solution.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises, and government agencies, and in over 100 countries, trust their information security needs to SafeNet.