Securing Digital Identities and Transactions in the Cloud

Security Guide

TRUSTED CLOUD FABRIC

SafeNet®

Securing Digital Identities and Transactions in the Cloud

SECURITY GUIDE

Features and Benefits:

Trusted Anchor with the Strongest Security in the Cloud

- Simplified secure access with client registrations
- Strongest security offering with a hardware-based approach to key management and security with convenience of remote management

Scalability for Future Cloud and Virtualization Environments

- Maximize investment and deployment with support up to 20 partitions and 100 clients
- Flexibility and ease of deployment as virtual and cloud environment grows

Lower Administrative Costs and Overhead

- Ease of management with elastic instancing capability for same virtual machine
- Maximum performance for cloud applications through high availability and load balancing features to deliver the reliability and scalability demanded by a virtualized infrastructure

The Key Vault: Leveraging Hardware Security Modules for Virtual Applications

Overview

Instead of spending thousands of dollars, and weeks, to install, customize, and integrate business transaction applications in-house on local servers and workstations, running these transactions 'in the cloud,' or on virtualized platforms, offers an attractive, simple, and cost-effective option.

In order to foster a level of trust matching that of existing internal enterprise resources, and to sustain compliance with internal policy and external regulations, it is essential that cloud platforms adopt a cryptographic deployment model. Through this adoption, organizations can ensure ownership and confidentiality of the cloud, integrity of business processes, transactional non-repudiation, and streamlined compliance with heightened security standards—without negatively impacting performance and reliability of cloud resources.

Leveraging the security of a centralized hardware security module, as the trust anchor in this cryptographic deployment model, is essential to managing cryptographic keys, access control, and other security policies. By deploying a hardware-based root-of-trust for key storage in a virtualized platform, organizations can securely perform the delivery of digital signing, encryption, access controls, secure key management, and a host of other capabilities within a hardware appliance in cloud environments. Armed with these capabilities, organizations can efficiently leverage the many benefits of cloud services and stay compliant with all pertinent regulatory mandates and security policies.

Combining the security benefits of hardware security modules with the cloud delivery model, security implementations can be far less expensive than traditional in-house deployments, putting state-of-the-art security capabilities within reach of even small- and medium-sized businesses for the first time.

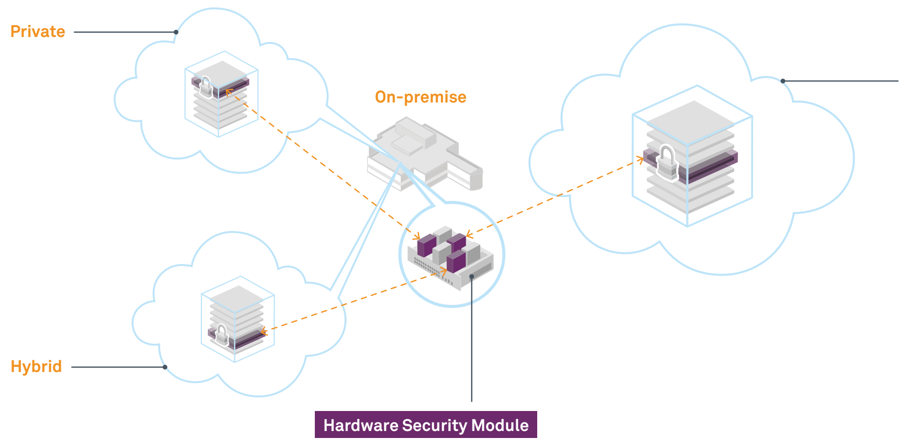
The Role of HSMs in the Cloud

Hardware Security Modules (HSMs) are critical in protecting high-value key material. HSMs deployed in the cloud act as a trust anchor for an enterprise's digital services, allowing security administrators to dictate policy based on business content, documents, and folders in order to ensure only authorized users and groups access sensitive data.

The HSM selected by an organization ultimately depends on the nature of their virtualized environment. One important differentiation to consider is keys in hardware versus keys in software. Many security professionals incorrectly assume that all HSMs store cryptographic keys within the confines of the HSM itself. In fact, while other leading HSMs generate their keys in hardware, they actually store the cryptographically wrapped keys on an application server. Storing cryptographic keys outside of an HSM introduces another surface of attack in which security polices could be manipulated or copied without the administrator's knowledge. This software approach actually eliminates the trusted anchor benefits provided by the HSM, opening the virtual cloud deployment up to vulnerabilities.

SafeNet offers the most advanced, keys-in-hardware, network-based HSMs, ideally suited for the demands of virtual and cloud infrastructures, offering FIPS- and Common Criteria-certified storage of cryptographic keys. SafeNet's HSMs, including SafeNet's Luna SA, offer an unparalleled combination of features—including central key and policy management, robust encryption support, flexible integration, and more—that form the basis for a secure cloud platform we define as Cryptography as a Service (CaaS). In addition, SafeNet is the only HSM solution provider to offer keys in hardware, ensuring that the cryptographic keys, paramount to securing your application and sensitive information, never leave the confines of the hardware appliance. Trusted security.

With this deployment, enterprise organizations can move their applications to the virtual cloud, while keeping their root-of-trust controlled and secure within the confines of their on-premise HSM. Ideally suited for virtualized infrastructures, enterprises can leverage Luna SA within this deployment with minimal interruption do to corporate firewalls as the HSM and cloud machines both live on the same virtual private network, through the use of a virtual private cloud (VPC) environment.



The Benefits of Cloud and Virtualization with SafeNet HSMs

Cryptography as a service enables providers to accommodate organizations needing a level of security previously unavailable in the cloud. By employing SafeNet HSMs enterprises, data centers and cloud providers can realize a range of benefits:

Trusted Security in a Virtual Environment

- **Secure Compartmentalization Through Partitioning.** By partitioning into separate security domains, the Luna SA can effectively compartmentalize a shared infrastructure to prevent unauthorized access to assets by other residents of a multi-tenant environment.
- **Secure Access with Multiple Client Registrations.** Luna SA uses industry-proven TLS with full client authentication to provide strong access controls and authorization for each client requesting HSM access. The Luna SA's comprehensive audit trail logs access and tracks changes to the HSM, providing a layer of accountability within a third party hosting environment.

Ease of management and implementation for lower administrative costs

- **Hardware-based Encryption with the Convenience of Remote Management.** The Luna SA PIN entry device (PED) offers a hardware-based trusted path, multifactor authentication method for its HSM partitions. In addition, the Luna PED can logically connect to an HSM across any network using a secured trusted path, eliminating the need for a skilled administrator at each site.
- **Ease of Virtualized Management with Elastic Instancing Capability.** The Luna SA's partitioning and client registration fully supports multiple instances of the same VM. A client's registration can be re-used multiple times concurrently so long as each instance resolves to the same host name (or IP address) from the Luna SA's perspective.

Scalability- a virtual solution that will grow with your business needs

- **Maximize Investment and Deployment with Support for up to 20 Virtual Machines.** A single set of Luna SA devices serve as the highly available HSM, partitioning into twenty separate security domains for virtual machines (VM). Up to 100 VMs can share any combination of these 20 security domains, including multiple instances of each VM.
- **VM Migration Support.** VM migration support is provided through the network-attached nature of the client-HSM connection. Because client machines are bound to specific HSM partitions a VM registered with a Luna SA can easily move to any virtualization server that still has network access to the Luna SA group.
- **Maximum Performance for Cloud Applications.** Luna SA has a high-availability and load-balancing mode that allows multiple Luna SA units to group as a logical set. This feature aids in the deployment of virtual services by delivering the reliability and performance required in a highly virtualized infrastructure.

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

©2011 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet.
All other product names are trademarks of their respective owners. ScG (EN)-02.10.11