THALES

SafeNet Luna PCIe HSM 7.1

PRODUCT OVERVIEW

Document Information

Product Version	7.1
Document Part Number	007-013578-003
Release Date	13 December 2019

Revision History

Revision	Date	Reason
Rev. A	13 December 2019	Initial release.

Trademarks, Copyrights, and Third-Party Software

Table 1: Third-party software used in this product

Software	License and copyright
editline	This product incorporates editline licensed under Apache v2.0 Open Software. Copyright 1992,1993 Simmule Turner and Rich Salz. All rights reserved. You can obtain the full text of the Apache v2.0 Open Software license at the following URL: https://www.apache.org/licenses/LICENSE-2.0
libFDT	Dual License Choice of BSD or GPL-2.0 Copyright (C) 2006 David Gibson, IBM Corporation.
libsodium	ISC License (ISCL) Copyright (C) 2013-2016
Linux Kernel	GPL-2.0
OpenSSH	This product uses a derived version of OpenSSH Copyright 1995 Tatu Ylonen , Espoo, Finland. All rights reserved . Copyright 1995, 1996 by David Mazieres . Copyright 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved You can obtain the full text of the OpenSSH license at the following URL: https://www.openbsd.org/policy.html

Software	License and copyright
OpenSSL	SSLeay License Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) OpenSSL license Copyright (C) 1998-2002 The OpenSSL Project
Software implementation of SHA2	Proprietary license Copyright (C) 2002, Dr Brian Gladman, Worcester, UK.
Software implementation of AES	Proprietary license Copyright (C) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for

direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

Regulatory Compliance

This product complies with the following regulatory regulations. To ensure compliancy, ensure that you install the products as specified in the installation instructions and use only Thales-supplied or approved accessories.

USA, FCC

This equipment has been tested and found to comply with the limits for a “Class B” digital device, pursuant to part 15 of the FCC rules.

Canada

This class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Europe

This product is in conformity with the protection requirements of EC Council Directive 2014/30/EU. This product satisfies the CLASS B limits of EN55032.

CONTENTS

PREFACE:
About the Product Overview

This document provides an overview of SafeNet Luna HSM suite of products. It contains the following chapters:

This preface also includes the following information about this document:

For information regarding the document status and revision history, see "Document Information" on page 1.

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN from the Technical Support Customer Portal at https://supportportal.gemalto.com.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Luna HSM users and security officers, key manager administrators, and network administrators.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only. It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This document uses standard conventions for describing the user interface and for alerting you to important information.

Notes

Notes are used to alert you to important or helpful information. They use the following format:

> **NOTE** Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. They use the following format:

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. They use the following format:

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

Command syntax and typeface conventions

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Dialog box titles (On the **Protect Document** dialog box, click **Yes**.) > Field names (**User Name**: Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{**a**|**b**|**c**} {<a>|<b>|<c>}	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and

workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).

CHAPTER 1:
The SafeNet Luna HSM

An HSM is a Hardware Security Module. HSMs are dedicated systems that physically and logically secure cryptographic keys and cryptographic processing. The purpose of an HSM is to protect sensitive data from being stolen by providing a highly secure operation structure. HSMs are fully contained and complete solutions for cryptographic processing, key generation, and key storage. They are purpose-built appliances that automatically include the hardware and firmware (i.e., software) necessary for these functions in an integrated package.

An HSM manages cryptographic keys used to lock and unlock access to digitized information over their life-cycle. This includes generation, distribution, rotation, storage, termination, and archival functions. An HSM also engages in cryptographic processing, which produces the dual benefits of isolation and offloading cryptographic processing from application servers.

HSMs are typically available in two forms:

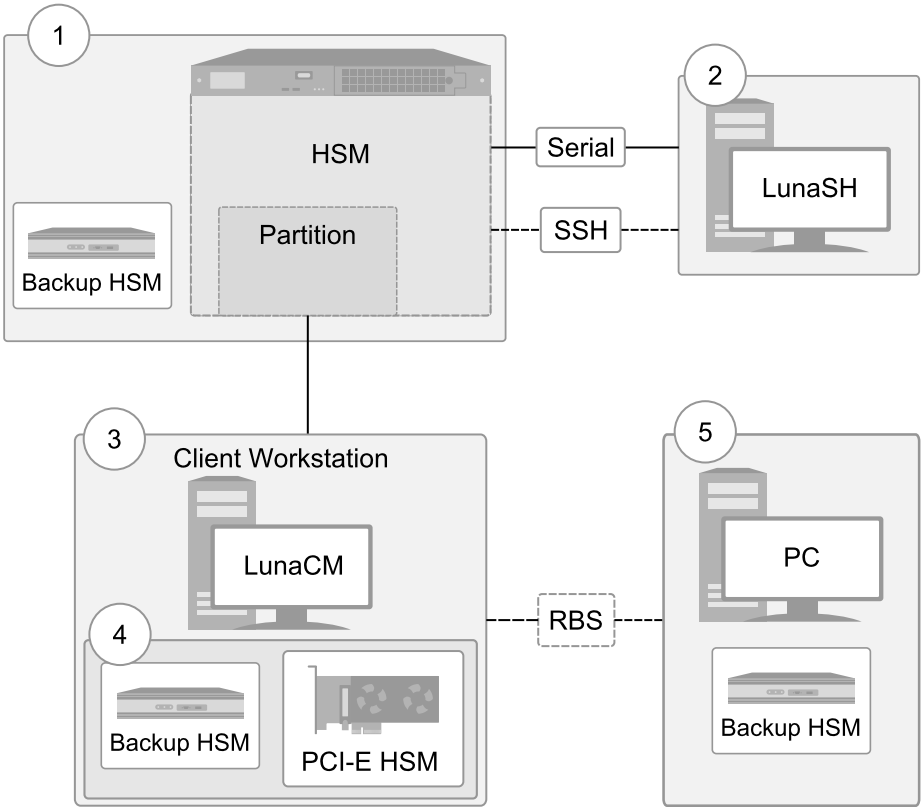
- Standalone network-attached appliances
- Hardware cards that plug into existing network-attached systems

These correspond to the "SafeNet Luna Network HSM" on the next page and "SafeNet Luna PCIe HSM" on page 13. There are several different HSM Series available for both types of HSMs each model is equipped with different performance capabilities to meet your needs.

For a high level overview of the distinctive features of the SafeNet Luna Network HSM and SafeNet Luna PCIe HSM, see "Features" on page 15

"HSM Connections" on the next page is a sample architecture, displaying potential connections between your SafeNet Luna HSM(s), server(s), and workstation(s). Some of the elements are optional configuration items, and might not be present in your system.

Figure 1: HSM Connections



1. Within your SafeNet appliance lies an HSM. That HSM holds one or more partitions that different users or clients can access.
2. Initial setup of your HSM requires you to connect directly to it via serial cable. Post-setup, you can use SSH to remotely access your HSM. Both of these connections use LunaSH, the command-line interface or shell for appliance and HSM configuration and management.
3. To perform cryptographic operations with your HSM or Partition, you must login remotely through the Luna client at your workstation. The client uses LunaCM for the configuration and administration of your Partition, and cryptographic APIs such as PKCS#11, Java, JCPROV, CSP, and KSP to perform significant operations.
4. The PCIe HSM is a small card that fits in your system's connector slots, and it is accessed directly through the Luna client at your workstation. The client uses LunaCM for the configuration and administration of your PCIe HSM, and cryptographic APIs to perform significant operations.
5. Backup HSMs are used exclusively to securely backup sensitive material from SafeNet Luna HSMs, and to restore backed-up material to SafeNet Luna HSMs. The SafeNet Luna Backup HSM can be connected to the primary HSM or to a server that can access the HSM. The Remote Backup Service (RBS) allows you to further remove your backup to a more remote location.

SafeNet Luna Network HSM

SafeNet Luna Network HSM stores, protects, and manages sensitive cryptographic keys in a centralized, high-assurance appliance, providing a root of trust for sensitive cryptographic data transactions. Deployed in more public cloud environments than any other HSM, SafeNet Luna Network HSM works seamlessly across your on-premises, private, public, hybrid, and multi-cloud environments. SafeNet Luna Network HSM is the most

trusted general purpose HSM on the market, and with market leading performance, true hardware-based security, and the broadest ecosystem available, SafeNet Luna Network HSM is at the forefront of HSM innovation.

Ethernet-attached

An Ethernet-attached HSM, SafeNet Luna Network HSM is designed to protect critical cryptographic keys and accelerate sensitive cryptographic operations across a wide range of security applications. It includes many features that increase security connectivity and ease-of-administration in dedicated and shared security applications.

Integrated Cryptographic Engine

The SafeNet Luna Network HSM can be shared between multiple applications or clients connected to it through a network. In the same way that mail and web servers provide email or web pages to authenticated clients, the SafeNet Luna Network HSM offers powerful key management and high-performance cryptographic processing to clients on the network. To achieve this, the SafeNet Luna Network HSM includes an integrated FIPS 140-2- validated HSM and the Cryptographic Engine, which offers the same high level of security as traditional HSMs. Additionally, the SafeNet Luna Network HSM adds a secure service layer that allows the Cryptographic Engine to be shared between network clients.

Partitions

The SafeNet Luna Network HSM also introduces the concept of HSM partitions, a feature that allows the SafeNet Luna Network HSM's single physical HSM to be divided into several logical HSM partitions, each with independent data, access controls, and administrative policies. HSM partitions can be thought of as 'safety deposit boxes' that reside within the Cryptographic Engine's 'vault'. The vault itself offers an extremely high level of security for all the contents inside, while the safety deposit boxes protect their specific contents from people who have access to the vault. HSM partitions allow separate data storage and administration policies to be maintained by multiple applications sharing one HSM without fear of compromise from other partitions residing on it. Each HSM partition has a special access control role who manages it. Depending on the configuration, each SafeNet Luna Network HSM can contain up to 100 partitions.

Dedicated Clients

HSM partitions can be dedicated to a single Client, or multiple Clients that share access to a single HSM partition. Clients are applications, or application servers, that connect to the SafeNet Luna Network HSM. Examples of possible clients are an encrypted database, a secure web server, or a Certificate Authority (CA); all these applications require the storage of sensitive cryptographic data or can benefit from the increased security and cryptographic performance offered by the SafeNet Luna Network HSM. Each Client is assigned to one or more specific HSM partitions. Clients authenticate to the SafeNet Luna Network HSM with a digital certificate and unique HSM partition challenge.

Employ the HSM as a Service

SafeNet Luna Network HSM empowers organizations to take a best practices approach to cryptographic key security by offloading cryptographic processes to a centralized, high-assurance key vault that can be deployed as a service. Only the SafeNet Luna Network HSM is able to provide trusted key owner ship and control, with full multi-tenancy across on-premises, private, public, hybrid, and multi-cloud environments.

SafeNet Luna PCIe HSM

SafeNet Luna PCIe HSM stores, protects, and manages sensitive cryptographic keys in a small form factor PCIe card, providing a root of trust for sensitive cryptographic data transactions. With SafeNet Luna PCIe HSM cryptographic processes are offloaded to a high-performance cryptographic processor. SafeNet Luna PCIe HSM easily embeds in servers and security appliances for an easy-to-integrate and cost-efficient solution for FIPS 140-2 validated key security. SafeNet Luna PCIe HSM benefits from a diverse feature set that enables greater centralized control through secure remote management, transport, and backup.

Single-partition

The SafeNet Luna PCIe HSM is a single-partition HSM card that you can embed in a pre-existing network-attached system. Access to the partition is managed by a special access control role. The SafeNet Luna PCIe HSM offers hardware accelerated ECC algorithms that can be used in the development of solutions for resource constrained environments (devices like smart phones, tablets, etc.), without the need to purchase additional licenses. ECC offers high key strength at a greatly reduced key length compared to RSA keys; higher security with fewer resources.

Cost Effective

Like in the SafeNet Luna Network HSM, the SafeNet Luna PCIe HSM securely stores cryptographic keys in its hardware; sensitive information never leaves the HSM. The SafeNet Luna PCIe HSM provides PKCS#11-compliant cryptographic services for applications running on the server in a secure and tamper-proof hardware package. Leveraging a SafeNet Luna PCIe HSM in your appliance or service represents a cost effective way to bring FIPS 140-2 and Common Criteria validated solutions to market.

SafeNet Luna PCIe HSM empowers organizations to take a best practices approach to cryptographic key security by offloading cryptographic processes to a dedicated small form factor cryptographic processor. SafeNet Luna PCIe HSM is the highest performing embedded HSM on the market.

Comparing the SafeNet Luna Network HSM Appliance and PCIe HSM

SafeNet Luna Network HSM Appliance	SafeNet Luna PCIe HSM
> Field-upgradable to 100 partitions > Includes hardened OS > High security, stable networking, and environmental protection via built-in chassis > Routine firmware and software updates > Automatic system logging	> Limited to 1 partition > Compatible with external OS: Windows, Linux > Allows custom and flexible chassis intrusion security > Routine firmware updates > Light and low-cost

A database server using an HSM would require one HSM, while a secure website using SSL on the same network would require a second, separate HSM. As the number of secure applications requiring an HSM grows, so does the number of ordinary HSMs deployed. The SafeNet Luna Network HSM bypasses this limitation by implementing multiple virtual HSMs, or HSM Partitions on a single HSM server. A PCIe HSM is useful for cases that need limited, but highly secure, data protection. A Network HSM and its appliance are useful for cases that require a more complex security infrastructure, like cloud computing.

SafeNet Luna HSM Models

Both the SafeNet Luna Network HSM and the SafeNet Luna PCIe HSM come in different models with different performance capabilities. Which one you choose to use will depend on your organization's security needs.

> **NOTE** The FIPS levels below indicate the standard to which the product is designed. Always confirm the HSM certification status before deploying an HSM in a regulated environment.

Luna A (Password-authenticated, FIPS Level 3)

Luna A models offer secure storage of your cryptographic information in a controlled and easy-to-manage environment. Luna A models protect your proprietary information by using password authentication. Depending on your needs, Luna A models are available at several performance levels, as follows:

Luna A700	> Standard performance > 2MB memory > SafeNet Luna Network HSM • Standard enclosure • 5 partitions
Luna A750	> Enterprise-level performance > 16MB memory > SafeNet Luna Network HSM • Standard enclosure • 5 partitions, upgradable to 20
Luna A790	> Maximum performance > 32MB memory > SafeNet Luna Network HSM • Standard enclosure • 10 partitions, upgradable to 100

Luna S (PED-authenticated, FIPS Level 3)

Luna S models offer secure storage of your cryptographic information in a controlled and highly secure environment. Luna S models protect your proprietary information by using multifactor (PED) authentication. Depending on your needs, Luna S models are available at several performance levels, as follows:

Luna S700	> Standard performance > 2MB memory > SafeNet Luna Network HSM • Standard enclosure • 5 partitions

Luna S750	> Enterprise-level performance > 16MB memory > SafeNet Luna Network HSM • Standard enclosure • 5 partitions, upgradable to 20
Luna S790	> Maximum performance > 32MB memory > SafeNet Luna Network HSM • Standard enclosure • 10 partitions, upgradable to 100

Luna X (PED-authenticated, FIPS Level 4)
Luna X models offer secure storage of your cryptographic information in a maximally secure and controlled environment. They are intended for use in hostile environments. Luna X models protect your proprietary information by using multifactor (PED) authentication. Depending on your needs, Luna X models are available at several performance levels, as follows:

Luna X700	> Standard performance > 2MB memory > SafeNet Luna Network HSM • Tamper Active enclosure • 5 partitions
Luna X750	> Enterprise-level performance > 16MB memory > SafeNet Luna Network HSM • Tamper Active enclosure • 5 partitions, upgradable to 20
Luna X790	> Maximum performance > 32MB memory > SafeNet Luna Network HSM • Tamper Active enclosure • 10 partitions, upgradable to 100

Features

SafeNet Luna HSMs perform an order of magnitude faster than their competition, and have a variety of features that distinguish them. These include:

Security
SafeNet Luna HSMs are manufactured to high security standards and are currently seeking FIPS Level 3 and Common Criteria certifications. SafeNet Luna HSMs protect your data from unwanted tampering with secure anti-intrusion and vulnerability detection mechanisms.

See "Security" on page 17 for details.

Redundancy and reliability
SafeNet Luna HSMs are equipped with physical features and configurations that enable auto-recovery of your HSMs.

See "Redundancy and Reliability" on page 22 for details.

Networking abilities
SafeNet Luna HSMs are compatible with NTLS and STC network connections. .

See "Networking" on page 1 for details.

User access control
SafeNet Luna HSM products offer multiple identities, some mandatory and some optional, that you can invoke in different ways to map to roles and functions in your organization.

See "User Access Control" on page 27 for details.

Different modes of authentication
SafeNet Luna HSMs are factory configured to be either password-authenticated or PED-authenticated, depending on the level of security you wish to protect your data with.

See "Authentication" on page 29 for details.

Capabilities and policies
SafeNet Luna HSMs, and partitions within them, are characterized by capabilities that are set at the factory or added by means of capability updates, and that are adjusted by means of settable policies that correspond to some of them.

See "Capabilities and Policies" on page 36 for details.

Flexible backups
SafeNet Luna HSMs contain sensitive material that, if lost, could be detrimental. The SafeNet Luna Backup HSM and RBS securely back up and store such information that can be restored in case of failures in primary HSM functioning.

See "Flexible Backups" on page 38 for details.

Logging and reporting
SafeNet Luna HSMs are equipped with performance monitoring and audit logging features to monitor security and provide audits of HSM activity.

See "Logging and Reporting" on page 41 for details.

CHAPTER 2:
Security

SafeNet Luna HSMs ensure the highest quality of protection of your cryptographic material with the following security measures:

> "Layered Encryption" below
> "Tamper Protection" on page 19
> "Certification" on page 20

Layered Encryption

SafeNet Luna HSMs do not keep any objects in the clear. All objects are encrypted by multiple layers, and are fully decrypted in temporary (volatile) memory only when needed.

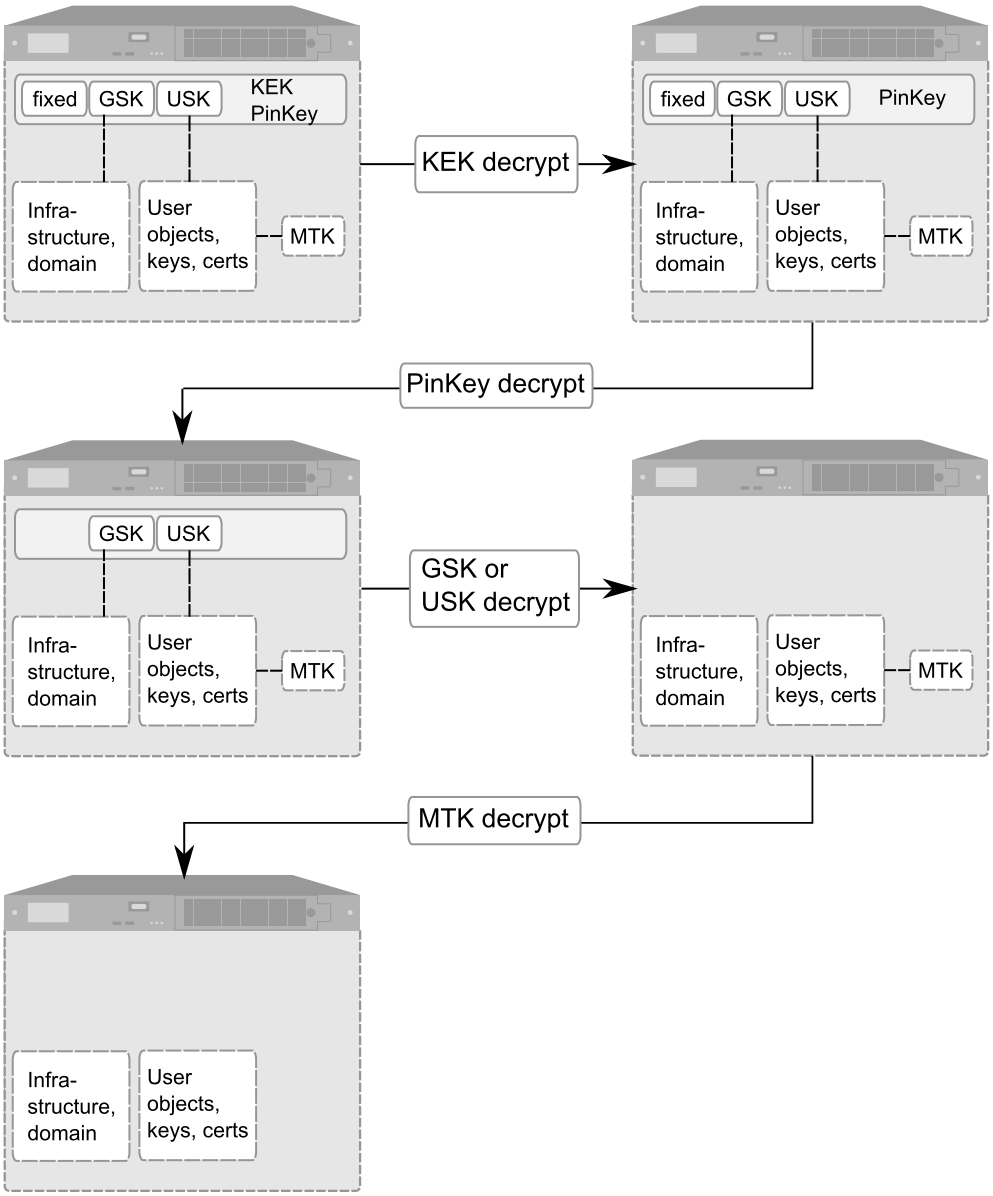
Hierarchy of Protection

One general storage key (GSK), for the HSM, protects general storage objects that might be needed by various roles. A separate user storage key (USK), for each role, protects the contents of the partition accessed by that role. The hierarchy of protection, depicted in "HSM Layered Encryption" on the next page, applies to each individual role. The USK for each role on the HSM encrypts objects that are owned by that role, ensuring that each person sees and touches only what belongs to them. Every SafeNet Luna HSM has a master tamper key (MTK) that strongly encrypts each object generated and stored within the HSM.

The key encryption key (KEK) further encrypts every key being used to ensure that your keys are never shown in plaintext.

Three-Layer Authentication Model

Figure 2: HSM Layered Encryption



When the HSM is powered on, everything is still tightly encrypted.

1. KEK is unique to each HSM, and encrypts everything that is encrypted by the PinKey.
2. During login, KEK and PinKey decryptions are performed.
   - For password-authenticated HSMs, the PinKey is the HSM SO password (or Partition SO, or CO or CU or Auditor, depending on who is logging in).
   - For PED-authenticated HSMs, the PinKey is the secret retrieved from the correct blue SO PED key (or black or gray or white, depending on who is logging in).
3. GSK encrypts all general-storage objects, while USK encrypts all security and user objects for the role logged into the HSM. Objects are decrypted individually when needed.

4. At the lowest level, MTK encrypts all objects.
5. Some objects are fully decrypted in volatile memory only when in use. Others, including ECDSA with NIST Prime curves, AES, DES3, and RSA keys remain MTK-encrypted. Once decrypted and accessible, objects inside the HSM can be used. If power is lost or a tamper occurs, all objects are tightly encrypted once again.

The in-depth application of multiple layers of security at all levels of the interface to SafeNet Luna HSMs and their internal HSMs provides a high degree of confidence that cryptographic material within the HSM will not be compromised. Customers with extremely demanding security requirements can enhance the already strong security of SafeNet Luna HSMs by choosing appropriate installation, HSM configuration, and policy options.

Cloning Domain

Every HSM or partition is part of a cloning domain, set at initialization time. Multiple HSMs or partitions can be set to be part of the same cloning domain or different ones. Key material cannot leave its cloning domain, so if an attacker were to try to copy your cryptographic material to a device that does not share a cloning domain with your HSM or partition, they would be unsuccessful. Using cloning domains ensures that key material can travel only between trusted and authorized devices. This adds a strong layer of defense against attackers.

> **NOTE** The cloning domain is not the lowest encryption level so a cloning operation does not provide access to Crypto material.
> Operations that use cloning are limited to backup, restore and synchronizing the HSMs in HA groups (among HSMs that share the same domain). Only the backup operation imposes a source-partition domain on the target partition within the Backup HSM; the restore operation and the HA synchronization both require that the source and target HSMs or partitions must already have matching domains.

Tamper Protection

Physical Security

SafeNet Luna HSMs are equipped with intrusion-resistant, tamper-evident hardware, and use the strongest cryptographic algorithms to ensure that your data is secure. If a security breach is detected, a tamper event occurs and the HSM becomes locked until the tamper is cleared by the appropriate authority or the HSM is reset.

SafeNet Luna PCIe HSM

The SafeNet Luna PCIe HSM, or cryptographic module, is a multi-chip standalone module as defined by FIPS PUB 140–2 section 4.5. This means that:

- The module is enclosed in a strong enclosure that provides tamper-evidence. Any tampering that might compromise the module's security is detectable by visual inspection of the physical integrity of the module. In addition, any attempts to physically tamper with the token would likely result in the destruction of its circuitry and components, thus ensuring that your keys and sensitive objects are safe from an attacker.
- The module's physical design also resists visual inspection of the device design, physical probing of the device and attempts to access sensitive data on individual components of the device.

If an attacker with unlimited resources were to simply steal the appliance, and apply the resources of a well-equipped engineering lab, it might be possible to breach the physical security. However, without the password (password-authenticated HSMs) or the PED keys (PED-authenticated HSMs), such an attacker would be unable to decipher any signal or data that they manage to extract.

With that said, it is your responsibility to ensure the physical security of the unit to prevent such theft, and it is your responsibility to enforce procedural security to prevent an attacker ever having possession of (or unsupervised access to) both the HSM and its authentication secrets.

Surrounding Environment

The data sheets provided by SafeNet show the environmental limits that the device is designed to withstand. It is your responsibility to ensure that the unit is protected throughout its working lifetime from extremes of temperature, humidity, dust, vibration/shock that exceed the stated limits.

We do not normally specify operational tolerances for vibration and shock, as the SafeNet Luna HSM is intended for installation and use in an office or data center environment. We perform qualification testing on all our products to ensure that they will survive extremes encountered in shipping, which we assume to be more demanding than the intended operational environment.

It is also your responsibility to ensure that the HSM appliance is installed in a secure location, safe from vandalism, theft, and other attacks. In summary, this usually means a clean, temperature-, humidity-, and access-controlled facility. We also strongly recommend power conditioning and surge suppression to prevent electrical damage, much as you would do for any important electronic equipment.

Authentication Data Security

It is your responsibility to protect passwords and/or PED keys from disclosure or theft and to ensure that personnel who might need to input passwords do not allow themselves to be watched while doing so, and that they do not use a computer or terminal with keystroke logging software installed.

Certification

FIPS

At any given time, a FIPS-validated version of the HSM is available, and a newer not-yet-validated version might also be available for newly introduced products that have not had time to go through the long evaluation and validation process. The usual practice is to ship units pre-loaded with the firmware and software at the FIPS-validated level by default, while providing the option to update the Client software, Appliance software, and HSM firmware to the newer version. This allows customers who need FIPS validation to have that configuration from the factory, and customers who need newer features (and do not need FIPS validation) to upgrade by simply installing the newer software and following the upgrade procedure. To check the progress of HSM versions that are submitted for FIPS 140-2 validation visit the NIST site at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

Common Criteria

Some versions of the product are submitted for Common Criteria EAL evaluation.

You can check SafeNet Sales or SafeNet Customer Support to inquire about certification status of SafeNet Luna HSM products. If FIPS validation or CC EAL certification are not requirements for you, then the newest version is normally the preferred option.

CHAPTER 3:
Redundancy and Reliability

SafeNet Luna HSMs are reliable in the case of unexpected events like power failures in the following ways:

- They have hot-swappable power supplies that can be replaced without turning off your system.
- They have dual fans to ensure that your HSM remains at a constant temperature and does not overheat and fail should one fan fail. This allows you to continue using your HSM while you replace the defective fan.

SafeNet Luna HSMs can also be grouped in a High Availability (HA) configuration for auto-recovery of your data in case an HSM fails. See "High Availability" below for an overview of this scheme.

High Availability

SafeNet Luna PCIe HSM products include the capability to group multiple devices into a single logical group – known as an HA (High Availability) group. Applications only see a virtual HSM that is a consolidation of all the HSMs in your HA group. Operations and key material from those HSMs are automatically synchronized to the application.

When an HA group is defined, cryptographic services remain available to the consuming applications as long as at least one member in the group remains functional and connected to the application server. In addition, many cryptographic commands are automatically distributed across the HA group to enable performance gains for many applications.

HSMs and appliances are unaware that they might be configured in an HA group. This allows you to configure HA on a per-application basis. The way you group your HSMs depends on your circumstances and desired performance. See "HA Configuration Overview" below.

Once you have set up an HA group, you can configure several options:

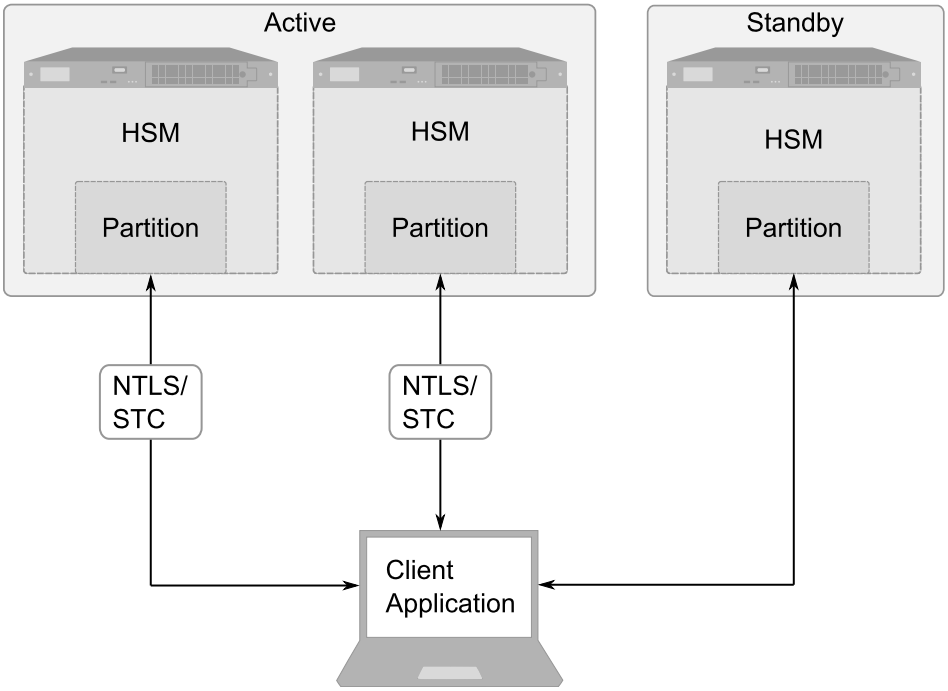
- "Standby Mode" on page 24
- "Load Balancing" on the next page
- "Failover" on page 24
- "Recovery" on page 25

The requirements for implementing High Availability are outlined in "Requirements" on page 25

HA Configuration Overview

As of SafeNet Luna HSM release 6.x, the SafeNet high availability function supports the grouping of up to thirty-two members. However, the maximum practical group size for your application is driven by a trade-off between performance and the cost of replicating key material across the entire group. The number of HSMs per group of application servers varies based on the application use case but, as depicted in "HA Sample Configuration" on the next page, groups of three are typical.

Figure 3: HA Sample Configuration



As performance needs grow beyond the performance capacity of three HSMs, it often makes sense to define a second independent HA group of application servers and HSMs to further isolate applications from any single point of failure. This has the added advantage of facilitating the distribution of HSM and application sets in different data centers.

Key Material Replication

Whenever an application creates key material, the HA functionality transparently replicates the key material to all members of the HA group before reporting back to the application that the new key is ready.

The HA library always starts with what it considers its primary HSM (initially the first member defined in an HA group). Once the key is created on the primary it is automatically replicated to each member in the group. If a member fails during this process, the key replication to the failed member is aborted after the failover time out. If any member is unavailable during the replication process (that is, the unit failed before or during the operation), the HA library keeps track of this and automatically replicates the key when that member rejoins the group.

Once the key is replicated on all active members of the HA group, a success code is returned to the application.

Load Balancing

The default behavior of the client library is to attempt to load-balance the application's cryptographic requests across the entire set of devices in the HA group. The top level algorithm is a round-robin scheme that is modified to favor the least busy device in the set. As each new command is processed, the SafeNet Luna PCIe HSM client looks at how many commands it has scheduled on every device in the group. If all devices have an equal number of outstanding commands the new command is scheduled on the next device in the list. However, if the devices have a different number of commands outstanding on them, the new command is scheduled on the device with the fewest commands queued. This modified round-robin has the advantage of biasing load away from any device currently performing a lengthy command.

The least-busy algorithm uses the number of commands outstanding on each device as the indication of its busyness.

Single-part vs. multi-part operations

In addition to this least-busy bias, the type of command also affects the scheduling algorithm. Single-part (stateless) cryptographic operations are load-balanced. Multi-part (stateful) commands that involve cryptographic operations are load-balanced.

However, key management commands and multi-part (stateful) commands that involve information retrieval are not load-balanced. Key management commands affect the state of the keys stored in the HSM. As such, these commands are targeted at all HSMs in the group. The command is performed on the primary HSM and then the result is replicated to all members in the HA group. Key management operations are infrequent for most applications. Multi-part operations carry cryptographic context across individual commands. The cost of distributing this context to different HA group members is generally greater than the benefit. For this reason multi-part commands are all targeted at the primary member. Multi-part operations are infrequent actions, so most applications are not affected by this restriction.

HA groups shared across servers

When an HA group is shared across many servers, different initial members can be selected while the HA group is being defined on each server. The member first assigned to each group becomes the primary. This approach optimizes an HA group to distribute the key management and/or multi-part cryptographic operation load more equally.

Standby Mode

By default all members in an HA group are treated as active. They are kept current with key material and used to load-balance cryptographic services. In some deployment scenarios it makes sense to define some members as standby. In this mode, only the active units are used for active load-balancing. However, as key material is created they are automatically replicated to both the active units and standby unit. In the event of a failure of all active members, the standby unit is automatically promoted to active status.

The primary reason for using this feature is to reduce costs while improving reliability. This approach allows remote HSMs that have high latency to be avoided when not needed. However, in the worst case scenario where all the active HSMs fail, the standby member automatically activates itself and keeps the application running.

Failover

A failover event involves dropping a device from the available members in the HA group. All commands that were pending on the failed device are transparently rescheduled on the remaining members of the group. When a failure occurs, the application experiences a latency stall on some of the commands in process (on the failing unit) but otherwise sees no impact on the transaction flow. The least-busy scheduling algorithm automatically minimizes the number of commands that stall on a failing unit during the twenty second timeout.

Lengthy commands

Most commands are completed within milliseconds. However, some commands can take extended periods to complete – either because the command itself is time-consuming (for example, key generation); or because the device is under extreme load. To cover these events the HSM automatically sends “heartbeats” every two

seconds for all commands that have not completed within the first two seconds. The twenty second timer is extended every time one of these heartbeats arrives at client, thus preventing false failover events.

Failure of the primary unit

If the primary unit fails, clients automatically select the next member in the group as the new primary. Any key management or single-part cryptographic operations are transparently restarted on a new group member. If the primary unit fails, any in-progress, multi-part, cryptographic operations must be restarted by the application.

As long as one HA group member remains functional, cryptographic service is maintained to an application no matter how many other group members fail.

Recovery

After a failure, the recovery process is straight-forward. Depending on the deployment, you can employ an automated or manual recovery process. In either case there is no need to restart an application.

Automatic Recovery

With automatic recovery, the client library automatically performs periodic recovery attempts while a member is failed. The frequency of these checks is adjustable.

The application does not restart.

Most customers enable auto-recovery in all configurations.

Manual Recovery

Simply run the client recovery command and the recovery logic inside the client makes a recovery attempt the next time the application uses the HSM. As part of recovery, any key material created while the member was offline is automatically replicated to the recovered unit.

Even if a manual recovery process is selected, the application does not need to be restarted.

Permanent failure

Sometimes a failure of a device is permanent. In this event, you only need to remove the failed unit and deploy a new member to the group. The running clients automatically resynchronize keys to the new member and start scheduling operations to it.

Requirements

The SafeNet HA and load-balancing features work on per-client and per-partition bases. This provides a lot of flexibility. For example, it is possible to define a different sub-set of HSMs in each client and even in each client's partitions (in the event that a single client uses multiple partitions). SafeNet recommends to avoid these complex configurations and to keep the HA topography uniform for an entire HSM. That is, treat HSM members at the HSM level as atomic and whole.

Network topography

The network topography of the HA group is generally not important to the proper functioning of the group. As long as the client has a network path to each member the HA logic will function. Keep in mind that having a varying range of latencies between the client and each HA member causes a command scheduling bias towards the low-latency members. It also implies that commands scheduled on the long-latency devices have a larger overall latency associated with each command.

In this case, the command latency is a characteristic of the network. To achieve uniform load distribution, ensure that latencies to each device in the group are similar (or use standby mode).

Member Configuration and Version

All members in an HA group have the same configuration and version. Running HA groups with different versions is unsupported. HSMs are configured identically to ensure smooth high availability and load balancing operations.

SafeNet Luna HSMs come with various key management configurations: cloning mode, key-export mode, etc. HA functionality is supported with both cloning and SIM variants – provided all members in the group have the same configuration. Clients automatically and transparently use the correct secure key replication method based on the group's configuration.

Physical and Virtual Slots

By default the client library presents both physical slots and virtual slots for the HA group. Directing applications at the physical slots bypasses the high availability and load balancing functionality. An application must be directed at the virtual slots to activate the high availability and load balancing functionality. A configuration setting referred to as HAonly hides the physical slots. SafeNet recommends using this setting to prevent incorrect application configurations. Doing so also simplifies the PKCS#11 slot ordering given a dynamic HA group.

Application developers should be aware that the PKCS#11 object handle model is fully virtualized with the SafeNet HA logic. The application must not assume fixed handle numbers across instances of an application. A handle's value remains consistent for the life of a process but it might be a different value the next time the application is executed.

For detailed instructions on setting up HA, see the *Administration Guide*.

CHAPTER 4:
User Access Control

Access to your HSM is controlled through implementation of HSM and partition-level users and roles. Some of these identities are mandatory, some are optional, and the way you use them is up to you and your organization.

A user is anyone who has access to the HSM or partition in question. A user can have one role associated with it, which grants the user certain access privileges. Different roles will allow the user to perform a different set of commands, depending on the role's function.

For detailed instructions on creating and initializing roles and users, see the *Administration Guide*.

HSM Level Users and Roles

Roles that access the HSM, the cryptographic engine within or connected to the host, include mandatory roles (see "Mandatory Roles" below) and optional roles (see "Optional Roles" on the next page).

Mandatory Roles	
HSM Security Officer (HSM SO)	HSM Administrator (HSM Only) > Initializes the HSM > Creates and deletes application partitions > Sets and changes global HSM Policies > Manages HSM-level backup and restore operations
Application Partition Security Officer (Partition SO) **Blue PED Key**	> Creates partition-level roles > Activates partition > Sets and changes partition-level Policies > Manages partition-level backup and restore operations > Resets passwords
Application Partition Crypto Officer (CO) **Black PED Key**	Shares same administrative capabilities as Partition SO, as well as > Creates and modifies cryptographic objects in the partition > Creates Crypto User role

NOTE The Partition Security Officer role is responsible for initial setup and maintenance of the partition, while the Crypto Officer is the partition owner who changes and manages its cryptographic objects.

Optional Roles	
Application Partition Crypto User (CU) **Grey PED Key**	Restricted read-only user > Uses cryptographic objects like encrypt/decrypt and sign/verify
Auditor **White PED Key**	> Manages HSM audit logging

In addition to the HSM roles listed above, certain other HSM-wide secrets exist for special purposes. Those include:

> Cloning domain (Red PED Key): determines whether the "cloning" (secure copy of cryptographic objects) operation is permitted between two HSMs (which must share identical domain secrets); cloning is used in some forms of backup, as well as in HA.

> Remote PED vector (Orange PED Key): for PED-authenticated HSMs only, permits establishing a secure path for the HSM to access remotely-located Luna PEDs and PED keys.

Partition Level Users and Roles

Independent application partitions are created by the HSM Administrator, but ownership and management of a partition falls on the separate Partition SO role.

For HSMs that contain multiple partitions, each partition acts as its own virtual HSM and has its own set of mandatory roles (see "Mandatory Roles" on the previous page), excluding HSM Administrator (HSM SO), and optional roles ("Optional Roles" below).

Optional Roles	
Application Partition Crypto User (CU) **Grey PED Key**	Restricted read-only user > Uses cryptographic objects like encrypt/decrypt and sign/verify
Auditor **White PED Key**	> Manages partition audit logging

In addition to the roles listed above, each HSM Partition requires:

> Cloning domain (Red PED Key): allows the secure copy of the partition's cryptographic objects to another partition (which shares an identical domain secret) in backup or HA operations.

> Remote PED vector (Orange PED Key): for PED-authenticated partition only, permits establishing a secure path for the HSM Partition to access remotely-located Luna PEDs and PED keys.

CHAPTER 5:
Authentication

Each SafeNet Luna HSM comes in one of two authentication types – Password authenticated or PED authenticated. The authentication type is configured at the factory and cannot be modified in the field.

For an outline of the key differences between password and PED authentication, see "Authentication Types" below.

Table 1: Authentication Types

Password Authentication	PED Authentication
Two-factor authentication not available	Two-factor authentication available by way of physical PED key per role and optional PED PIN per key
Authentication can be input locally or from a remote terminal	Authentication requires physical local connection or pre-configured remote PED link
Knowledge of partition password sufficient for accessing cryptographic keys	Access to cryptographic keys restricted to CO (read/write) and CU (read only), possession of appropriate PED key(s) and potentially their PED PINs required
Dual or multi-person access control not available	Dual or multi-person access control available by way of MofN (split-knowledge secret sharing)
Key-custodian responsibility and role separation linked to password knowledge only	Key-custodian responsibility and role separation linked to partition password knowledge and PED key(s) ownership

For more detailed information on each authentication type, see:

> "Password Authentication" below
> "PED Authentication" on page 31

Password Authentication

In general, there are two paths to access the SafeNet appliance and its HSM:

> The administrative path, via SSH or via local serial link, which uses the LunaSH command-line interface
> The client path, via SSL, by which client applications use the SafeNet Luna Network HSM API to perform cryptographic functions within pre-assigned virtual HSMs (called partitions) on the SafeNet system

For SafeNet Luna HSMs with Password Authentication, the various, layered roles are protected by passwords.

HSM Admin

To access the HSM to perform HSM-specific administration tasks (set HSM-wide policies, update firmware and capabilities, backup and restore the HSM, create and remove HSM Partitions, etc.), you must be logged in to LunaSH as admin, then you must further be logged in as HSM Admin (of which there can be only one per SafeNet Luna HSM). Good security practices suggest that the HSM Admin password should be different from the appliance admin password. However, your corporate policies may differ. As the HSM Admin, you can connect locally, via a serial terminal, or remotely via SSH – you must first be logged in as admin to have access to LunaSH commands.

Partition Owner

To access HSM Partitions, in order to perform partition-specific administration tasks (set partition-specific policies, assign Partition to Clients, revoke Clients, etc.), you must be logged in to LunaSH as admin, then you must further be logged in as Partition Owner (of which there can be several - one for each partition in the HSM) , using the Partition Password. Good security practices suggest that the Partition Password should be different from the appliance admin password, different than the HSM Admin password, and different than other Partition Passwords (for other partitions). However, your corporate policies may differ. As the Partition Owner, you can connect locally, via a serial terminal, or remotely via SSH – you must first be logged in as admin to have access to LunaSH commands.

Client

To access HSM Partitions with an application to perform cryptographic operations on data, you must connect remotely via SSL (called NTLS in our implementation) as a Client (one that has been registered by certificate exchange and assigned by the Partition Owner to this partition), then pass a User-type (this is done invisibly by your client application), and present the Partition Password (also done automatically by your application). The password used by a Client is the same Partition Password that is used by the Partition Owner for the particular partition. What limits the scope of operations that a registered, authenticated Client can perform on a partition is the fact that partition administrative commands can be issued only via LunaSH. Thus, for security, Clients must not be allowed to learn the appliance admin password that gives access to LunaSH.

Authentication

Objects on the HSM are encrypted by the owner of the HSM Admin space or of the User space (partition), and can be decrypted and accessed only by means of the specific secret (password) imparted by the HSM Admin or the partition User respectively.

If you cannot present the secret (the password) that encrypted the objects, then the HSM is just a secure storage device to which you have no access, and those objects might as well not exist.

> **NOTE** The administrative role secret is also the application-authentication secret: one plain-text secret used for two purposes. On a Password-authenticated HSM, once the administrator (Crypto Officer or Crypto User) has distributed the secret to the application(s), the only way to restrict access by applications (or personnel) that have come into possession of that secret is to change the password - which also changes the authentication for the associated administrative role.

Advantages

Using password authentication, as opposed to PED authentication, has the following advantages:

- Convenience: changing passwords and authentication secrets is easy in the case of personnel changes or suspected compromise
- Direct mapping to organizational policies: password change policies already existing in an organization are easy to map onto a password authenticated framework

Disadvantages

Passwords are less secure than the two-factor authentication provided by the PED, and thus have the following disadvantages:

- Vulnerability to observation: passwords being typed can be easily observed in person, through a camera, or with mal-ware like keystroke loggers
- Record-keeping: secure passwords are obscure and must be written, with its record securely stored
- Accountability: it is difficult to know who might have seen or been told a password

PED Authentication

The connection between the Luna PED and the SafeNet Luna HSM is a secure trusted path.

- For the SafeNet Luna Network HSM, the PED connection is on the appliance front panel.
- For the SafeNet Luna PCIe HSM, the PED connection is a slot-edge connector, directly on the HSM card, accessible at the exterior of a tower or server computer (not through the host computer).

For Local PED, the connection is a secure physical link, directly to the HSM, bypassing the computer memory and bus.

For Remote PED, the PED Key information is made available from the PED location by a PedServer instance, and is received at the HSM location by a PedClient instance there. Two connection options are available:

- standard, or client-initiated Remote PED involves the PedClient reaching out to a PedServer; while the path is clear, the PED Key data is encrypted and secured at both ends by the Remote PED Vector (on an orange PED Key and in the HSM)
- peer-to-peer, or server-initiated Remote PED involves the PedServer instance reaching out to the PedClient instance, in order to satisfy HSM location behind a firewall that forbids outgoing initiation of connections; the PED Key data is secured at both ends by the Remote PED Vector (on an orange PED Key and in the HSM), and the network connection is secured by a TLS link, using previously exchanged certificates.

At no time does an authentication secret exist in-clear, anywhere in computer memory or on any computer bus.

In general, there are three paths to access the SafeNet Luna HSM:

- The administrative path, via SSH or via local serial link, which uses the LunaSH command-line interface
- The Client path, via TLS (our implementation is called NTLS), by which client applications use the SafeNet Luna HSM API to perform cryptographic functions within pre-assigned virtual HSMs (called Partitions) on the HSM
- The Trusted Path, used for authentication data passed from the PED and PED keys - this path ensures that HSM authentication data does not pass unencrypted through a host or terminal computer, where it might be subject to attack

For SafeNet Luna HSMs with PED Authentication, the various layered roles are protected by a combination of PED keys and passwords.

HSM Admin (Security Officer)

To access the HSM to perform HSM-specific administration tasks (set HSM-wide policies, update firmware and capabilities, backup and restore the HSM, create and remove HSM Partitions, etc.), you must first be authenticated as SO (Security Officer) or HSM Admin (of which there can be only one per SafeNet Luna HSM). The authentication data for SO/HSM Admin is a secret carried on a blue PED key. For the SO to login and issue HSM commands, someone must be present at the connected local Luna PED, or at the configured Remote Luna PED, to insert the required blue PED key when prompted. Otherwise, HSM commands cannot be used.

Partition User (Crypto Officer)

To access HSM Partitions to perform partition-specific administration tasks, such as setting partition policies, assigning partitions to clients, or revoking clients, you must be authenticated as Partition User. There can only be one Partition User per HSM on the SafeNet Luna PCIe HSM, or there can be several on the SafeNet Luna Network HSM - one for each partition. The authentication data for the CO (Crypto Officer) or Partition User is both a password and a secret carried on a black PED key. As the Partition User/CO, you can connect locally, via a serial terminal, or remotely via SSH. To perform partition administration on SafeNet Luna Network HSM, you must first be logged in as admin to have access to LunaSH commands.

- For the SafeNet Luna PCIe HSM, you simply need access to the host computer, where you can use LunaCM commands. For the Partition User/CO to login and issue partition administration commands, someone must be present at the connected Luna PED (or the configured and validated Remote PED) to insert the required black PED key when prompted, or the partition must have been left in Activated state.
- For the SafeNet Luna Network HSM, good security practices suggest that the Partition Password be different than the appliance admin password, and different from other Partition Passwords.

If you have invoked the Crypto Officer/Crypto User distinction, there are two Partition Passwords, but only the Crypto Officer password allows you to run LunaSH or LunaCM commands to administer the partition. It is also recommended that the passwords for each of these roles differ.

Client (Crypto User)

To access HSM Partitions with an application to perform cryptographic operations on data, you must pass a User-type (this is done invisibly by your client application), and present the Partition Password (also done automatically by your application).

- For a standard "Client", the password is the same Partition Password that is used by the Partition User for the particular partition. What limits the scope of operations that a registered, authenticated Client can perform on a partition on a SafeNet Luna Network HSM is the fact that partition administrative commands can be issued only via LunaSH. Thus, for security, Clients should not be allowed to learn the appliance admin password that gives access to LunaSH command line. For SafeNet Luna PCIe HSM, the password or other authentication that gives access to the client application is often the same authentication that gives access to LunaCM for partition administration, so the ability to keep roles separate is more dependent on control of PED keys.
- For a Crypto User client, the password is different from the Crypto Officer password, offering another layer of protection for the partition and its contents.

Auditor
This role combines a special, limited-access appliance account and a special HSM role authenticated by the white PED key, for the purpose of managing HSM audit logs. The auditor is distinct and separate from other role on the appliance and the HSM, conforming to the requirements of auditing standards.

Remote PED

By default, Luna PED is connected directly to the HSM via a USB cable, and powered by the included power block. However, Luna PED can also be used remotely from the HSM(s) for which it manages access control. When it is not convenient to be physically near the host computer that contains a SafeNet Luna HSM you can operate remotely and securely.

The PED-Authenticated SafeNet Luna HSM, and one or more orange PED keys are imprinted with a Remote PED Vector (RPV). This can occur at any time before the HSM is deployed, and requires a locally connected PED. All future PED and PED key interactions can then be accomplished distantly from the HSM, as follows:

1. One computer, running a supported OS, hosts the HSM. This could be:
   - A server or tower containing a SafeNet Luna PCIe HSM.
   - A SafeNet Luna Network HSM appliance.

   The HSM host computer must be network attached. HSM administration commands can be input locally, or via remote connection, but the network connection is essential for Remote PED operation.
2. A second computer (laptop, workstation, server running a supported Windows version) has a Luna PED (Remote Capable) attached via USB, and powered via its included power block. The Remote PED host computer must be network attached. The administration of the distant HSM host does not have to come from this Remote PED host computer, but it is usually done that way, since the person handling the PED must coordinate with the person giving commands to the HSM.The Remote PED host computer and PED must have the orange Remote PED Key (RPK) available, along with:
   - Either blue, black and red (optionally, white) PED keys that were imprinted with the HSM previously
   - Or blank blue, black, and red (optionally, white) PED keys that are about to be imprinted along with the HSM
3. The HSM is told to look to a remote PED for its authentication requests.
4. The PED host computer has the LunaPED driver installed, and runs the pedserver utility.
5. The HSM host computer runs the pedclient utility, and the HSM is told to connect to the Remote PED.
6. The Remote PED (via the pedserver) receives the request and prompts for the orange PED Key.

   The Remote PED and the HSM (via the pedclient/pedserver connection) must agree that the provided orange PED key contains the same Remote PED Vector as the one imprinted on the HSM, and only then is the secure Remote PED link is established.
7. The HSM SO runs commands on the HSM (on the host computer) via remote desktop or SSH connection.

All future authentication for the HSM can be performed at the Remote PED, with no need for personnel to visit the HSM host, which could be locked away in a lights-off facility on the other side of the world.

Authentication

Objects on the HSM are encrypted by the owner of the HSM Admin space (rarely) or of the User space (partition), and can be decrypted and accessed only by means of the specific secret injected from the blue PED key (HSM Admin) or the black PED key (User) respectively.

If you cannot present the secret (the PED key) that encrypted the objects, then the HSM is just a secure storage device to which you have no access, and those objects might as well not exist.

Challenge Secrets

When the HSM is PED-authenticated:

- The administrative role secret contained on a black or gray PED key is one secret, used only by administrative personnel.
- The challenge-secret or password is a second secret (plain text, initially presented on the PED screen, but you can change it), which is the application-authentication secret, that allows the HSM verify that the presenting application is entitled to perform cryptographic operations on the particular application partition.

The application can submit its own authentication (that second secret) only after the PED key secret has "opened" the HSM partition for operation (by Activating it). That is, there are two levels of protection: one administrative, and the other operational, where the operational level is gated by the administrative level.

Activation

By default, PED-authenticated partitions require that a PED key and challenge password be provided each time a user or application authenticates to the HSM. For some use cases, such as key vaulting, the need to provide a physical key to access the HSM may be desirable. For most application use cases, however, requiring a physical key each time the application accesses the HSM is impractical.

Activation allows registered users and applications to authenticate to the HSM without a PED key, using only a challenge secret. The PED key secret for the CO or CU role is copied the first time you perform an action that requires authentication, and it is cached on the HSM.

The ability to use activation is determined by its corresponding policy. Enabling this policy will allow you to use activation.

Auto-Activation

In the event of a restart or short power outage, activated roles are deactivated and must re-authenticate with a PED key and challenge secret.

Auto-activation enables automatic re-activation of an activated role, so that users or applications do not have to provide a PED key again to reactivate their role.

The ability to use auto-activation is determined by its corresponding policy. Enabling this policy will allow you to use auto-activation.

Advantages

Using PED authentication, as opposed to password authentication, has the following advantages:

- Security: no written record of the secret or password exists, so it cannot be compromised
- Tracking: access and handling of physical devices (PED keys) can be tracked and controlled
- Duplication restrictions: duplication and promulgation can be prevented by physical security measures

> Physical device: using the PED to input passwords and PEN PINs prevents key-logging exploits that typed passwords are vulnerable to

Disadvantages

PED keys are physical items that can be lost or misplaced, unlike passwords, and thus have the following disadvantages:

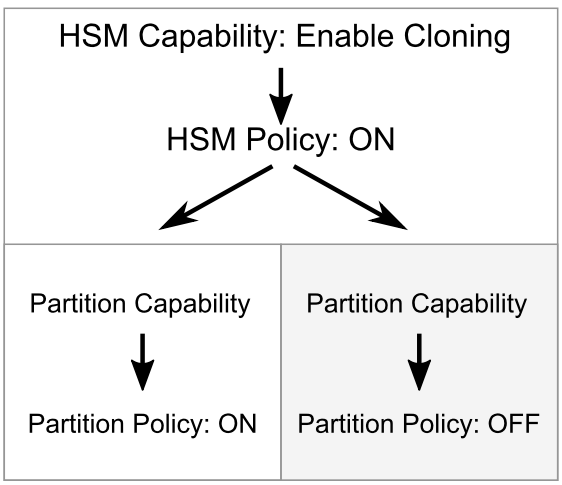
> Password change policies: scheduled or mandated password-change cycles in an organization can be logistically intensive when HSMs share PED key secrets

> Inconvenience: handling of secrets requires hands-on, physical action by personnel to perform changes of authentication secrets in case of compromise

CHAPTER 6:
Capabilities and Policies

HSMs, and partitions within them, are characterized by capabilities that are set at the factory, or added by means of capability updates, and that are adjusted by means of settable policies that correspond to some of the capabilities. HSM capabilities, and the HSM policies that derive from them, apply HSM-wide. Application partition capabilities, and the application partition policies that derive from them, can be inherited from the HSM, or control characteristics that make sense only at the application partition level. "Capability and Policy Inheritance" below illustrates an example of how capabilities and policies can be inherited from the HSM-level to the partition-level on a SafeNet Luna Network HSM.

Figure 4: Capability and Policy Inheritance



All policies have an equivalent capability, but not all capabilities are matched by a policy that allows adjustment of the capability. The HSM administrator is responsible for setting up the HSM with capabilities, but it is up to the Partition SO to enable their corresponding policies.

Some policy settings are numerical values that can be increased or decreased. Most policy settings are simply OFF/ON switches. Policy setting requires that the SO be logged in. For HSM-wide policies, that is the HSM SO. For partition-level policies, that is the Partition SO.

Set Policies

Set policies with the **hsm changepolicy** command or the **partition changepolicy** command, as appropriate. The command requires that you identify the policy number that is to change, and the new value it is to hold. For OFF/ON policies, the value is set as zero or one, respectively.

For detailed lists of HSM and Partition capabilities, as well as their corresponding policy settings, see the *Administration Guide*.

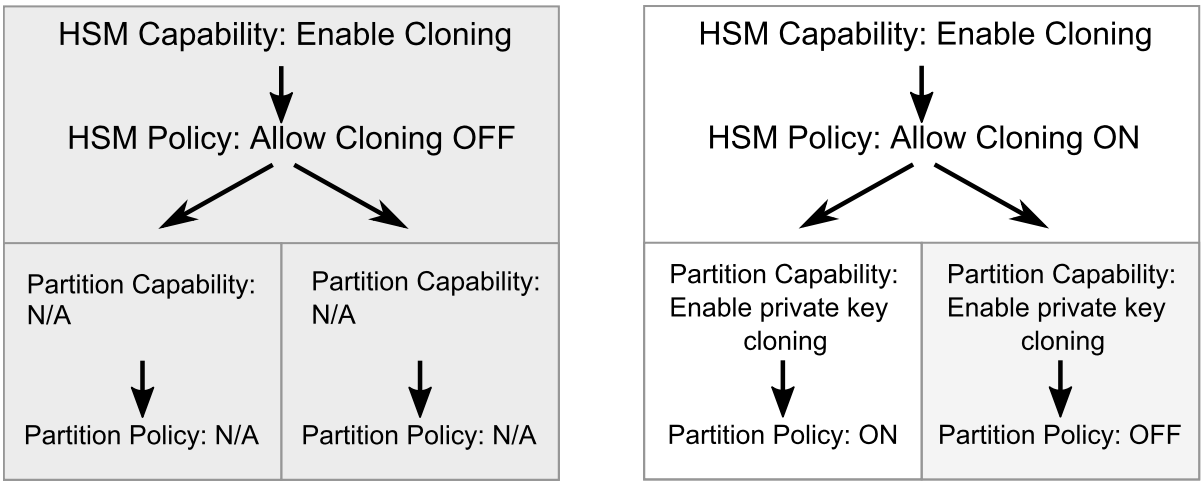
Example: Cloning

The cloning operation allows you to duplicate or copy the contents of your HSM or partition to other HSMs or partitions that share a cloning domain. The HSM capability that controls cloning on your HSM is Enable Cloning. The equivalent HSM Policy, Allow Cloning, is the modifiable switch that turns cloning on or off for your specific HSM.

> **NOTE** Turning cloning ON or OFF is destructive, and resets your HSM. Ensure that you decide early on in your configuration whether or not you will be using this capability.

"Cloning Capability Inheritance" below shows how the cloning capability is inherited by partitions within your HSM, depending on whether you turn it on or off when you set its policy value.

Figure 5: Cloning Capability Inheritance



If cloning is not allowed HSM-wide, then no partition on the HSM will be able to use cloning.

If cloning is allowed HSM-wide, then each partition inherits that capability and can independently decide whether it wants to enable it.

CHAPTER 7:
Flexible Backups

While some applications might deal in ephemeral objects that are erased after their use, in many SafeNet Luna HSM applications the keys and objects within the HSM and partition have value and are meant to persist. For such valuable data, any security regime requires that the data be backed up in secure fashion, and stored securely.

Backup and restore operations require access to the objects in your partition in order to copy them. As such, backup and restore operations are restricted to HSMs that share a cloning domain and partitions whose administrators allow access to.

Backup

Backup operations copy the secure material on your HSM and store it on a separate Backup HSM. Backup is not performed continuously. The frequency of backup is dependent on your backup plan or strategy.

The SafeNet Luna Backup HSM can be connected directly to the HSM to perform backup or restore operations on the spot. It is not able to perform cryptographic operations; it functions only in its secure backup/restore role. The Backup HSM takes on the authentication type of the primary HSM with which it is paired for backup - so it becomes a password-authenticated Backup HSM when backing up a password-authenticated primary HSM, and a PED-authenticated Backup HSM when backing up a PED-authenticated primary HSM.

The Backup HSM can also be connected to a host computer, located at a distance from the source HSM, and can perform backup and restore operations over secure network connection. This is normally the case when the source HSM is kept in a secure server room or a lights-out facility.

There are several ways to do backup with SafeNet Luna HSMs. Depending on the type and number of HSMs and partitions you have, and how they are organized, different methods may be more suitable for your situation. The following sections describe these methods in more detail:

> "Local Backup" below

> "Remote Backup" on the next page

> "Comparing Local Versus Remote Backup" on page 40

Restore

Restore operations are only necessary if there is no hope of recovering your data on your HSM, and using your backup to restore the content is the only solution. The restore operation is identical to the backup operation, only in the opposite direction.

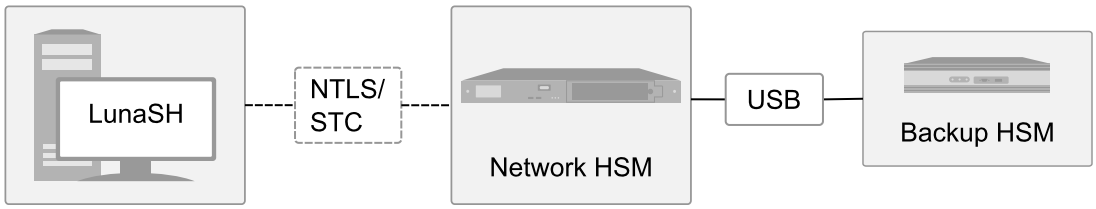
Local Backup

Local backup requires a direct connection to the HSM to be successful. Backup can be done directly from the secure appliance housing the HSM or from a client workstation connected to the HSM.

Centralized Local Backup

Centralized backup uses a direct connection between the HSM you wish to back up and the Backup HSM. "Centralized Local Backup" below outlines the basic setup required for simple local backup.

Figure 6: Centralized Local Backup

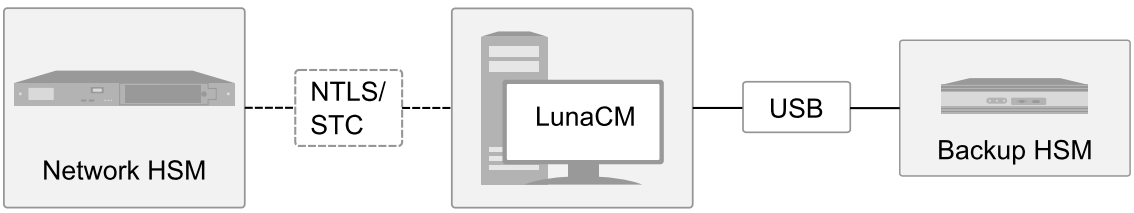


Connecting your Backup HSM directly to the HSM or secure appliance housing the HSM you wish to back up is a highly secure method of copying your keys. It requires you to have physical access to the HSM in addition to the HSM SO and Partition SO credentials for every partition needing backup. The backup operation is initiated from the LunaSH command line.

Client-side Local Backup

Client-side backup connects to the HSM you wish to back up via your client workstation. The Backup HSM connects directly to the client workstation to perform backup. "Client-side Local Backup" below outlines the basic setup required for local backup via client workstation.

Figure 7: Client-side Local Backup

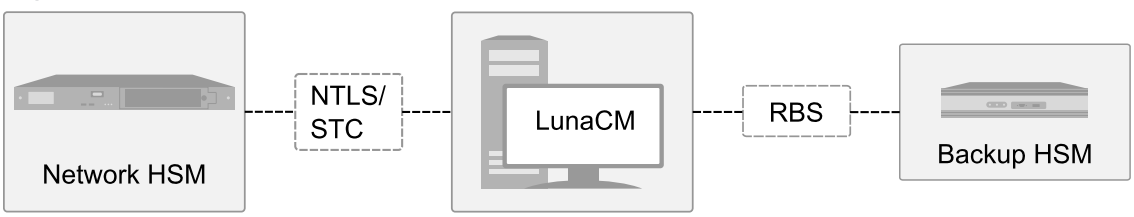


The backup operation in this case is still local, and thus requires a direct wired connection between your Backup HSM and client workstation. This method is highly secure, and allows for some flexibility in case the HSM you wish to back up is not easily available for direct connection. A PC running Luna Client and LunaCM can connect to the HSM and, with the appropriate Partition SO credentials for every partition needing backup, can access and securely copy your cryptographic keys.

Remote Backup

Remote backup allows you to securely back up your HSM from any location that is convenient. A secure network connection facilitated by RBS enables you to access your HSM or partition without needing to be physically near it. "Remote Backup" below outlines the basic setup required for remote backup.

Figure 8: Remote Backup



Remote Backup Service (RBS) runs on a system hosting a SafeNet Luna Backup HSM, making the Backup HSM available to distant HSMs. This allows backup and restore operations to run from any location most convenient for the administrator. In this configuration, backup and restore operations are performed over secure network connection.

Comparing Local Versus Remote Backup

Regardless of whether you use a local connection to backup and restore your HSM, or whether you use a remote one, backup and restore operations always require a Backup HSM. How you decide to connect it and organize your backup/restore infrastructure depends on what your organization needs.

Local backup is easier and faster to configure than remote, but the remote option allows more secure storage of your cryptographic material in case the entire environment in which your HSM resides collapses.

For detailed instructions on carrying out backup and restore operations, see the *Administration Guide*.

CHAPTER 8:
Logging and Reporting

SafeNet Luna PCIe HSM allows you to track and report all activity on your HSM to encourage responsibility, ensure accountability, and upkeep tight security.

Both SafeNet Luna Network and PCIe HSMs come equipped with HSM-level audit logging via Audit role. See "HSM-Level Audit Logging" below.

The SafeNet Luna PCIe HSM also includes appliance-side audit logging and services that monitor your HSM's performance. See "Appliance-Level Performance Monitoring" below.

HSM-Level Audit Logging

Monitoring HSM activity is essential to maintaining a high level of security for the highly sensitive material on your HSM. SafeNet Luna HSMs have logging and reporting abilities to support this. These features are implemented in the HSM firmware for maximum security.

Logging

Secure logging is done at the whole HSM level. The HSM stores a record of past operations that is suitable for security audit review. Audit logging sends HSM log event records to a secure database on the local file system, with cryptographic safeguards ensuring verifiability, continuity, and reliability of HSM event log files.

Each log entry indicates what event occurred when, and who initiated it. Critical events are logged automatically.

Audit Management

For circumstances that require more comprehensive review of events taking place on the HSM, an HSM-level Audit role (White PED key for PED-authenticated HSMs) can be used. Each HSM has a unique Audit role whose purpose is to manage audits and monitor HSM activity.

The Audit role is independent from the other roles on the HSM. Creating the Audit role does not require the presence of the HSM SO and if the Audit role is initialized, the HSM and partition administrators are prevented from working with the log files. Only the Auditor can add failures, successes, key usage, and other events to the HSM logging procedure.

Audit log integrity is ensured against altering log records. Separating logging and its role from other administrative roles protects critical information related to the operations of your HSM.

For detailed instructions on implementing audit logging, see the *Administration Guide*.

Appliance-Level Performance Monitoring

SafeNet Luna HSMs monitor their own conditions for issues that might require administrative attention. Appliance-side logging of HSM activity moves HSM logging directly into the appliance file system. The purpose is to record HSM operations while bypassing the resource-heavy in-HSM log security features. Like at the

HSM-level, appliance-level logging and auditing are split into separate services and roles. Only the Auditor on the appliance can engage in audit management. The Audit role is separate from Admin, Operator, and Monitor.

Appliance performance monitoring can be done via LunaSH, SafeNet Crypto Command Center, or SafeNet REST-API. LunaSH allows you to specify commands yourself, while the latter two provide a friendly user interface to query the appliance.

Syslog

Syslog is a standard logging facility that writes messages it gets from the appliance to organized log files.

When a sensor reading on the appliance changes by an amount that crosses a configured threshold, the appliance will generate log messages according to their severity. These logs can be checked and accessed by an audit user.

SNMP

SafeNet Luna HSMs also support remote monitoring of conditions on a local HSM via SNMP (Simple Network Management Protocol). Should the condition of your HSM change in a way that requires your attention, SNMP will alert you via trap notification. Condition changes can include changes in memory or CPU usage, network connection status, and some environmental variables.

You can configure SNMP according to your organization's preferences; it is a flexible and optional feature. SNMP is secure and efficient, ensuring that faults in your HSM are detected early and that your cryptographic information remains safe.

For detailed instructions on implementing SNMP, see the *Administration Guide*.