SafeNet PCIe HSM 6.2.1

Product Overview

gemalto
security to be free

Document Information

Product Version	6.2.1
Document Part Number	007-011329-010
Release Date	26 July 2016

Revision History

Revision	Date	Reason
A	26 July 2016	Initial release.

Trademarks, Copyrights, and Third-Party Software

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the University of California, Berkeley and its contributors.

This product uses Brian Gladman's AES implementation.

Refer to the End User License Agreement for more information.

Disclaimer

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

Gemalto 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 Gemalto 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.

Gemalto 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 Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto 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 Gemalto-supplied or approved accessories.

USA, FCC

This device complies with Part 15 of the FCC rules. Operation is subject to the following conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Note: 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. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications not expressly approved by Gemalto could void the user’s authority to operate the equipment.

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 2004/108/EC. Conformity is declared to the following applicable standards for electro-magnetic compatibility immunity and susceptibility; CISPR22 and IEC801. This product satisfies the CLASS B limits of EN 55022.

CONTENTS

PREFACE
About the Product Overview

This document provides an overview of SafeNet 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 2

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 for this release at the following location:

- http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-2-1.pdf

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCIe HSM

Old product name	New product name
Luna G5 HSM	SafeNet USB HSM
Luna PED	SafeNet PED
Luna Client	SafeNet HSM Client
Luna Dock	SafeNet Dock
Luna Backup HSM	SafeNet Backup HSM
Luna CSP	SafeNet CSP
Luna JSP	SafeNet JSP
Luna KSP	SafeNet KSP

Note: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Audience

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

All products manufactured and distributed by Gemalto 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

Contact method	Contact	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support Provides access to the Gemalto Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
The SafeNet HSM Product Line

This chapter provides an overview of the SafeNet HSM product line. It contains the following sections:

SafeNet HSM Products - Overview

Gemalto SafeNet HSMs are hardware security modules designed to protect critical cryptographic keys and to accelerate sensitive cryptographic operations across a wide range of security applications. All SafeNet HSMs enable separation of roles by distinguishing between the HSM Security officer space (an administrative function) and the application Partition or User space, where client keys and objects are secured, and where client-invoked cryptographic operations take place. SafeNet HSMs fall into three categories:

- SafeNet PCIe HSM is a card-type HSM that installs into the PCIe slot(s) of a host computer. Multiple SafeNet PCIe HSMs can coexist in one host system. Each SafeNet PCIe HSM supports one HSM partition.

  See "About SafeNet PCIe HSM" on page 22.
- SafeNet USB HSM is a desktop HSM unit that connects locally to a host computer via USB interface. Multiple SafeNet USB HSMs can be linked via USB connection. Each SafeNet USB HSM supports one HSM partition.
- SafeNet Network HSM is a self-contained, network attached HSM appliance, containing an HSM card similar to SafeNet PCIe HSM, and normally resides in an equipment rack in a server room (often of the "lights off", unattended variety), and is accessed remotely via secure administrative and client links. Each SafeNet Network HSM supports multiple HSM partitions, the number governed by purchased licenses.

HSM Basics

An HSM is a Hardware Security Module. It has storage, cryptographic, and access-control functions, that allow cryptographic operations to be performed and segregated within a secure physical hardware boundary, while offloading such functions from the general-purpose pathways of the host or client. Here are basic elements common to SafeNet HSMs:

Volatile and non-Volatile Data Storage

SafeNet HSMs can contain both volatile and non-volatile data.

- Non-volatile data includes identification parameters and data objects (such as keys and certificates) that you wish to store for long-term re-use. Those objects persist on the HSM until you explicitly destroy or overwrite them. Non-volatile objects are encrypted.

- Volatile data is any data that should not persist when it is not in use. Volatile (or session) data disappears when the HSM loses power, or when a session closes. Volatile data includes decrypted copies of non-volatile objects.

Keys and objects are stored under multiple layers of encryption (see "HSM General Authentication Model" on page 61), and are decrypted within the physical bounds of the HSM, only into volatile/session storage, and only while being used. Any event that removes power to the HSM instantly erases volatile objects.

Initialization

SafeNet HSMs must be initialized before you can use them for the first time (or after an event that zeroizes the HSM, like too many consecutive failed login attempts on the Security Officer (SO) account).

Initialization establishes several HSM parameters, including identification and authentication of HSM Administrator or Security Officer (SO) and application Partition Crypto Officer and Crypto User who then have access to create and use HSM/Partition objects (keys, certificates, encrypted data, etc.).

Many applications from PKI and other cryptographic product vendors do not include the capability to initialize a SafeNet HSM, so SafeNet supplies the Lunacm utility program on all supported platforms, to perform that function and other maintenance functions.

Once a SafeNet HSM is initialized, no one can access it unless they provide the passwords or keys that unlock that specific HSM or Partition.

You can re-initialize a SafeNet HSM at any time (as SO). Re-initialization destroys all data on the HSM.

Authentication methods

SafeNet HSMs are factory configured to be either:

- Password authenticated - uses typed text strings to access the HSM and authenticate to all roles on the HSM; advantage, greater convenience.
- PED authenticated - uses physical tokens, called PED Keys, mediated by a PIN Entry Device, or PED, to access the HSM and authenticate to all roles on the HSM; advantage, greater security.

An HSM in the field cannot be changed from Password-authenticated to PED-authenticated, or from PED-authenticated to Password-authenticated. The only exception is the SafeNet Backup HSM, which configures itself at the time of a backup operation, to match the authentication scheme of the HSM being backed up - the Backup HSM performs Backup and Restore only, and has no ability to perform cryptographic operations

Separation of Roles and Functions

SafeNet HSM architecture includes several elements that allow or enforce separation of roles and functions.

Application Partition(s) Separate from HSM Administration Partition

The HSM Administrator or Security Officer (SO) presides over administrative tasks and responsibilities that affect the entire HSM. Those tasks include:

- setting policies that control all aspects of the HSM
- creating separate spaces for everyday cryptographic operations by your client applications
- creating and managing other roles and major functions

One of those functions is to create a defined, virtual HSM within the HSM, called an application partition for client objects (keys, certificates, etc.) and cryptographic operations. Until recently, that application partition was created by the HSM SO (a.k.a. "Administrator"), and remained under the control of the HSM SO, who then delegated daily

operations to a Partition Owner or Crypto Officer, who might, in turn delegate read-only operations to a Crypto User entity.

The SafeNet USB HSM and SafeNet PCIe HSM products support one application partition, each.

The SafeNet Network HSM appliance product supports multiple application partitions per HSM, with appropriate licensing.

The approach described above (sometimes referred to as 'legacy-type' partition configuration in these documents), where any application partition is owned by the HSM SO, is still available for customers who are accustomed to it and wish to continue with that scheme.

Partition Security Officer

Beginning with HSM firmware 6.22.0, with the Per-Partition SO capability applied, the HSM SO has the option to create an application partition with its own Security Officer. Once it is created, the partition is handed over completely to its new owner (the Partition SO) and the HSM SO has no further contact with it or control over it, except to delete it from the HSM at some future time if that becomes necessary.

The PPSO approach (see "Ownership of Application Partitions" on the next page) provides more emphatic separation of client cryptographic operations from overall HSM management. A PPSO partition is created empty. The Partition SO creates his/her own role by first initializing the application partition from within. The Partition SO fine-tunes the environment within the application partition by adjusting partition-specific policy settings, then creates the Crypto Officer role, and hands that responsibility to another person. This keeps management and operational tasks separate within the application partition, which in turn is untouched by the HSM SO.

This approach applies separately to multiple application partitions on an HSM that supports more than one application partition. Each such partition is private from the others, and from the HSM SO.

Separate Encryption of Material by Operational Roles and Functional Secrets

A role like HSM SO or Partition SO authenticates to the HSM or to a partition, gaining access to objects within by temporarily opening a layer of encryption until logout occurs, or the current session closes.

A cloning domain is a secret applied to an HSM or to an application partition, whereby secure copying of HSM or partition objects can take place only to/from another HSM or partition that has the same domain applied. If two containers have different cloning domains and a cloning operation is attempted, it simply fails when that decryption is attempted. The cloning domain governs backup-restore operations, and HA synchronization.

The MTK is an internal HSM key that encrypts almost every object on the HSM, and which is destroyed when a hardware tamper event (physical intrusion, or excursion beyond acceptable environmental parameters) or a software tamper event occurs. Two components of that key are kept in separate locations and can reconstitute the MTK to allow recovery from tamper. The SRK is an external holder for one of those components, that allows the bearer to control the manner and timing of official response to a tamper event.

The Remote PED vector is one of the few items not encrypted under the MTK, and allows the secure connection of a SafeNet PED device (see "About Remote PED" on page 35) to the HSM, from a remote location.

The Auditor is a role whose only purpose is to manage the HSM's audit logs, outside the control of any other entity.

Each of the above roles and functional secrets can be held by different persons in your organization, for the maximum separation of roles and activities with respect to the HSM. Alternatively, one person could be assigned more than one role (and given the authentication for each) if that conforms to your organization's security policy.

Historical Note

The product name "Luna" was taken from the name of the SafeNet moth, to conform with the originating company name "Chrysalis-ITS". The company name was derived from the hidden or secret existence of the moth as it developed within its cocoon, or the chrysalis. This was evocative of the hidden world of cryptography. Other moth names were considered for additional product lines, but the "Luna" brand very quickly achieved marketplace recognition and efforts were aligned under that brand.

After years of growing success with the SafeNet brand in the cryptographic marketplace, Chrysalis-ITS was acquired by SafeNet. Because the brand was well recognized and respected in the HSM marketplace, SafeNet maintained it.

Our SNMP MIB is still called CHRYSALIS.

Ownership of Application Partitions

Beginning with firmware 6.22.0, SafeNet HSMs support two modes of ownership of an application partition in the HSM.

Who is in Charge?

Per-Partition SO (PPSO)

- The application partition is entirely owned and controlled by its own Security Officer.
- The HSM SO can create or delete application partitions, but has no ability to see or touch contents.
- The uninitialized partition can be handed off to a person who is not associated with the HSM SO, and who can create the Partition SO identity without assistance from the HSM SO. On a Password-authenticated HSM, this means that the Partition SO can set and manage a partition SO secret that is not known by the HSM SO. On a PED-authenticated HSM, it means that the Partition SO can authenticate to the application with a blue PED Key that is completely unrelated to the blue PED Key used by the HSM SO.
- Only the application Partition SO can create the Crypto Officer. On a Password-authenticated HSM, this is an administrative role with its own text-string secret, but that secret must also be shared with any application that performs creative and destructive crypto operations. On a PED-authenticated HSM, the Crypto Officer authenticates with a black PED Key, and provides a text-string secret that is used by any application that performs creative and destructive crypto operations (like keygen, deletion of keys, etc.).
- Only the Crypto Officer can create the Crypto User. On a Password-authenticated HSM, this is an administrative role with its own text-string secret, but that secret must also be shared with any application that performs read-only crypto operations. On a PED-authenticated HSM, the Crypto User authenticates with a gray PED Key, and provides a text-string secret that is used by any application that performs read-only crypto operations (like sign/verify).

Legacy application partition

- The application partition's Security Officer is the Security Officer of the HSM (also called the HSM Administrator).
- The HSM SO can create or delete application partitions, and can see the objects in the application partition.
- The HSM SO creates the Crypto Officer (also known as the Partition Owner or User).
- The HSM SO creates the Crypto User, if desired.

The Legacy option is the default, and is the way SafeNet HSMs have worked in the past. This option applies for new, and for upgraded HSMs until you install firmware 6.22.0 or newer, and install the PPSO Capability Update. That is, if you do not update the HSM firmware, and do not also install the PPSO Capability Update, then your HSM works as previously.

The PPSO functionality requires new "role" commands in Lunacm. Those commands are not visible if the HSM firmware version is earlier than 6.22.0. Some of those commands are visible if you update the firmware to version 6.22.0 or newer, but most do not become functional until you also apply the PPSO Capability Update.

PPSO Feature Benefits and Limitations in a Nutshell

The PPSO feature is very useful if you have need of it, but is not for everyone.

Note: Terminology note -- "Partitions" refer to virtual HSMs within the physical HSM; "slots" refer to PCKS#11 cryptographic slots. SafeNet Shell (lunash) on the SafeNet Network HSM considers application partitions as partitions when they are created, and as partitions when they are used. The client-side lunacm (on computers running SafeNet HSM Client software) considers application partitions as partitions when they are created, and as slots when they are managed and when they are used by customer applications. The terminology might switch back and forth depending on which point of view is indicated, but they are all HSM partitions - logically and cryptographically insulated, and generally independent (with some caveats), virtual HSMs.

Benefit:

- PPSO is a building block to support multi-tenant HSM services, where, for example, multiple PKCS#11 slots can be used and managed by different organizations accessing one SafeNet Network HSM.
- Separation of roles is enhanced by separating management of application partitions from management of the overall HSM.

Limitations:

- Secure logging is done at the whole HSM level. Currently, there is no per-slot audit logging ability.
- The PPSO capability is applied at the whole HSM level. Only policies (not capabilities) can be changed on a per-slot (per-partition) basis. For example, you cannot mix Password-authenticated (a.k.a. FIPS2) and PED-authenticated (a.k.a. FIPS3) partitions/slots on the same SafeNet Network HSM.
- RPED (Remote PED) applies to the whole HSM. All partition owners/slot-holders share the same RPV (Remote PED Vector, or orange PED Key). If one slot owner changes the RPV, all other slot owners are no longer able to make the Remote PED connection.
- Most HSM commands are parallelized, which means that PED operations on one partition do not interfere with crypto operations on any other partition on the same HSM. As well, operations on the same partition tend not to interfere. Some exceptions exist, such as Delete operations, which must lock objects while the operation occurs.
- The Partition SO cannot be added to any pre-existing slots. A customer who has created the maximum number of partitions afforded by the currently applied license must either delete some partitions or purchase a larger license CUF (Capability Update File or Secure Package).
- The ability to create partitions with their own SOs (PPSO) adds some overhead to partition structure. Because the partition overhead is part of the user storage space, customer might need to shrink the storage usage per partition (by deleting some objects) in order to upgrade to firmware 6.22.0 or newer.

- The Audit role is destroyed by factory reset. The HSM administrator (or HSM SO) can issue the factoryReset . This means that the auditor is at the mercy of HSM SO even though he is supposed to audit the HSM SO activities as well.

Customer impact:

- All partitions, pre-existing or new, will have HSM generated serial numbers once the HSM is upgraded to firmware 6.22.0 (or newer). Customer's existing applications or administrative tools/procedures might need to be adjusted accordingly.
- Slot enumeration changes (see "Slot Numbering and Behavior" on page 1).

About SafeNet Network HSM

The SafeNet SafeNet Network HSM is an Ethernet-attached HSM (Hardware Security Module) Server designed to protect critical cryptographic keys and to accelerate sensitive cryptographic operations across a wide range of security applications. SafeNet Network HSM includes many features that increase security, connectivity, and ease-of-administration in dedicated and shared security applications.

SafeNet Network HSM comes in one of two model families, according to the level of authentication and access control. Your SafeNet Network HSM was factory configured to operate as either:

- a Password Authenticated version, equivalent to FIPS 140-2 level 2, using passwords, only, for authentication and access control
- a PED (Trusted Path) Authenticated version, equivalent to FIPS 140-2 level 3, that requires SafeNet PED and PED Keys for authentication and access control.

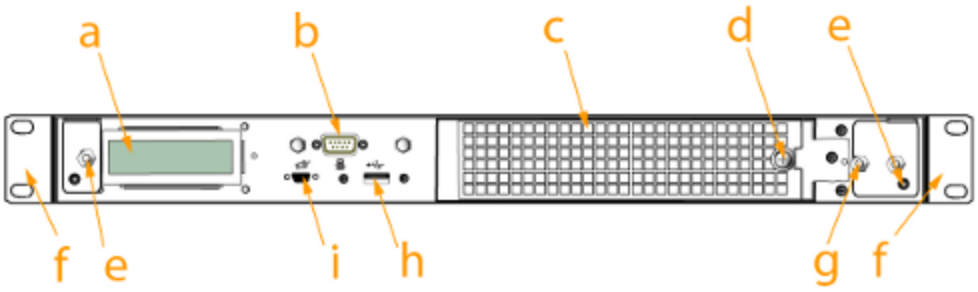
Physical Features

The standard appliance is the 1U-high, rack-mount device:

Here are some of the important physical features of the SafeNet Network HSM appliance.

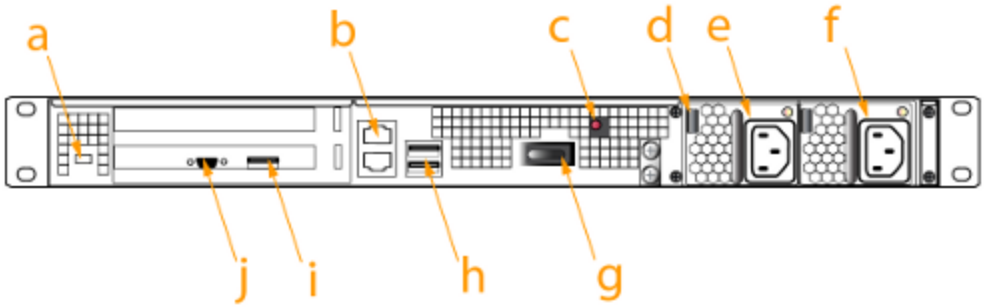
Front View

First, the front; this illustration shows the appliance with its snap-on decorative bezel removed...



Item	Name	Description
a	LCD system status screen	Shows IP info and scrolls through system status messages
b	Serial (console) port	Local connection for initial setup, and for admin account reset (local-only action for security reasons)
c	Ventilation-fan filter cover	Removable bracket allows cleaning of air filter
d	Fan filter cover retaining screw	A captive thumb-screw (no tool needed).
e	Mounts for removable front bezel	The decorative/protective front bezel mounts on the appliance front panel. Spring clips behind the bezel engage the mounting posts at the left and right ends of the appliance front panel.
f	Rack-mount tabs (removable)	Use these on the front, and the sliding tabs toward the rear to support your SafeNet appliance in a compatible equipment rack
g	Securing screw for fan bay	Torx screw secures the fan bay; opening to swap fan modules triggers a tamper event on the appliance
h	USB port	Use to connect SafeNet Remote Backup HSM (for backup of your HSM partition contents), SafeNet USB HSM, or SafeNet DOCK 2 (for PKI and for migration of cryptographic material from older backup token HSMs); same as USB port on back panel
i	PED port	Attach SafeNet PED 2, Pin Entry Device, reads the hardware (iKey) authentication devices for Trusted Path (FIPS 140 level 3) access control

Rear View



Item	Name	Description
a	Kensington Security Slot	Attach an industry-standard locking cable for additional physical security.
b	Ethernet ports	For network connection of your SafeNet appliance.
c	Decommissioning button	Recessed for safety; renders HSM contents unusable.
d	Power supply release tab	Press tab to release the catch, and slide the power supply out.
e	Removable power supply	One of two redundant power supplies.
f	Second removable power supply	The other of two redundant power supplies.
g	Start/stop switch	Use to stop the system if the command-line shutdown is not available; use to restart the system if it has been switched off.
h	USB ports	Use to connect SafeNet Remote Backup HSM (for backup of your HSM partition contents), SafeNet USB HSM, or SafeNet DOCK 2 (for PKI and for migration of cryptographic material from older backup token HSMs); same as USB port on front panel.
i, j	Unused ports	These ports are not used for SafeNet Network HSM; we recommend that you do not remove the covers that were installed at the factory.

FIPS and Common Criteria Validations and Certifications

At any given time, a FIPS-validated version is available (except for newly introduced products that have not had time to go through the year-long evaluation and validation process), and a newer not-yet-validated version might also be available. 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).

Similarly, some versions of product are submitted for Common Criteria EAL evaluation.

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

SafeNet HSM Cryptographic Engine

The SafeNet HSM's integrated SafeNet-Luna Cryptographic Engine is used to perform cryptographic operations and provide secure storage for sensitive cryptographic keys.

The SafeNet Cryptographic Engine enables the SafeNet Network HSM functionality by providing:

- secure cryptographic storage,
- cryptographic acceleration (up to 7000 1024-bit RSA signings per second),
- administrative access control and
- policy management.

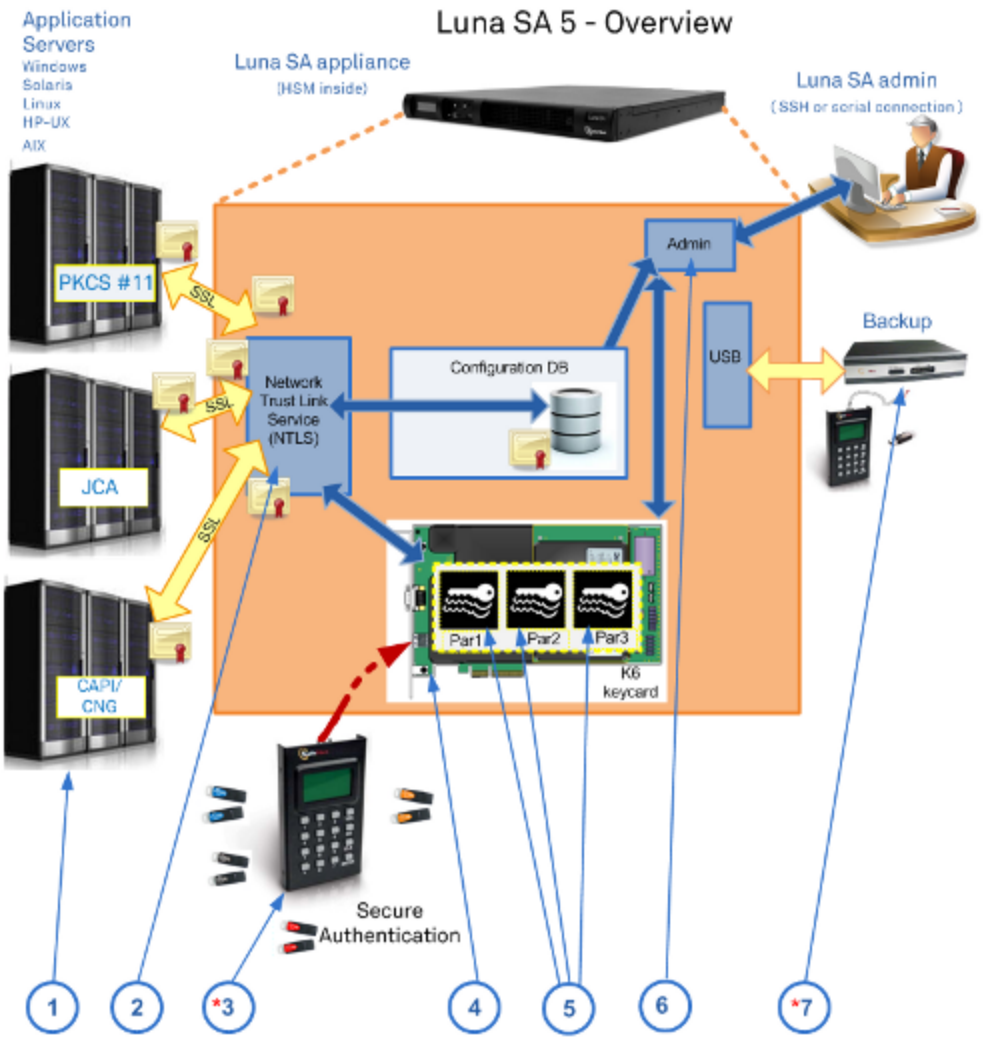
The SafeNet Cryptographic Engine can also be used in conjunction with the optional Trusted Path Authentication feature to provide FIPS 140-2 Level 3 validated HSM operation. That option is factory-configured and not subject to change in the field.

The SafeNet Network HSM Appliance

HSMs, in general, are designed to provide dedicated cryptographic functionality, including key generation, key storage, and digital signing, on a one-to-one basis to their host applications. For example, 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.

SafeNet Network HSM bypasses this limitation by implementing multiple virtual HSMs, or HSM Partitions on a single HSM server. Partitions are accessed via a Network Trust Link.

The following block diagram is a conceptual overview of the SafeNet Network HSM Server depicting internal systems, communications, and interaction with application servers.



SafeNet Network HSM operations encompass seven major elements. Some of these elements are optional configuration items, and might not be present in your system:

1. Server(s) hosting your client applications that need to create, store, and use crypto objects on an HSM application partition.
2. Network Trust Link. You can optionally use a Secure Trusted Channel (STC) link to add an extra layer of security for client-partition network links.
3. PED (trusted path) authentication
4. SafeNet K6 HSM Cryptographic Engine
5. HSM Partitions
6. Secure command line interface
7. Secure backup HSM

(* The Secure Backup HSM, and SafeNet PED (Trusted Path Authentication and Access Control) are options that might not be included with your system.)

About SafeNet PCIe HSM

The SafeNet HSM Customer documentation uses "SafeNet PCIe HSM" whenever it refers to either of the performance versions - SafeNet PCIe HSM 1700 or SafeNet PCIe HSM 7000, without need to specifically identify one version. Those two versions are so-named because their tested performance at repetitive RSA 1024-bit signings per second (under laboratory conditions was near one or the other of those numbers (1700 or 7000).

1024-bit RSA keys are actually outdated for most applications, due to their small size. However 1024-bit RSA signing has been an industry-standard way to convey application and HSM performance for many years and will continue to be used until an industry consensus is reached for an updated indicator.

HSM Basics

An HSM is a Hardware Security Module. An HSM stores cryptographic objects (keys, certificates, etc.), creates and destroys crypto objects, and performs cryptographic operations (encrypt, decrypt, sign, verify, wrap, unwrap) using those objects within the secure physical confines of the HSM - not exposed on a computer file system. The HSM also controls access to its contents and its functions.

The SafeNet PCIe HSM Cryptographic Module is an HSM. Here are the basic elements common to SafeNet HSMs:

Volatile and non-Volatile Data Storage

SafeNet HSMs can contain both volatile and non-volatile data:

- Non-volatile data includes identification parameters and data objects (such as keys and certificates) that you wish to store for long-term re-use. Those objects persist on the HSM until you explicitly destroy or overwrite them.
- Volatile data is any data that should not persist when it is not in use. Volatile (or session) data disappears when the HSM loses power.

The Card

The SafeNet PCIe HSM 5 [K6] HSM card is designed to the PCIe 1.1 standard, for use in PCIe x4 slots. The HSM card can be used in larger connector slots (from x4 up to x16).

Some x16 slots are intended by the computer motherboard manufacturer to be used for video cards, and might not work correctly with SafeNet PCIe HSM 5. The symptom is that, at start-up, the system detects a card in the slot, but the card does not respond as a video card, and so the system stops booting. This could happen to any non-video PCIe card inserted in such a slot. If you encounter a problem, try another available slot. Modern motherboards tend to support PCIe 2.0 standard, which is backward compatible with 1.1, when correctly implemented.

Of the three major vendors of PCI bridge chips (including the one that we used), each has known problems either of performance, compatibility, or both. Due to the variety of systems and component combinations in the market, we are unable to test with all possible platforms. At the time that this Help was written we found greater incompatibility among server systems than among desktop/workstation systems. If you encounter a problem that is not solved by moving the SafeNet PCIe HSM 5 card, contact SafeNet Technical Support -- e-mail: support@safenet-inc.com or phone 800-545-6608 (+1 410-931-7520 International).

Power

Power consumption for the SafeNet PCIe HSM card is rated at 12 Watts maximum, 8 Watts typical.

Partition

SafeNet PCIe HSM is a versatile HSM capable of many roles. Part of that versatility is achieved by separating HSM management (the Security Officer or HSM Admin space) from HSM operation (the User or client). This is achieved by means of the HSM partition or virtual HSM within the physical HSM.

The owner of the partition:

- can see and manage the contents of the partition, and
- can enable or disable access by client applications as desired, entirely separately from the overall HSM management performed by the SO.

The SO:

- can perform HSM updates/upgrades,
- can modify operating parameters
- can deal with tamper events,
- can create or destroy a partition, reset the authentication of an existing partition (when someone forgot his password or lost his PED Key, or someone has left the organization ... or been fired...),
- can authorize the creation of a partition challenge secret, and
- can perform other global operations without ever being able to see or touch the contents of the User/Owner's partition.

The roles are kept separate.

Initialization

SafeNet HSMs must be initialized before you can use them for the first time (or after an event, like too many consecutive failed login attempts on the SO account, which zeroizes the HSM). Initialization establishes several HSM parameters, including identification and authentication of HSM Security Officer (SO) and HSM Partition User who then have access to create and use HSM/Partition objects (keys, certificates, encrypted data, etc.). Once a SafeNet HSM is initialized, no one can access it unless they provide the passwords or keys that unlock that specific HSM or Partition. Initialization is meant to be performed only once on an HSM, and it erases any Authentication Data, and data or token objects contained on the token. Once the HSM is in use, be sure to avoid mistakenly initializing it again.

You can re-initialize a SafeNet HSM at any time (as SO). Re-initialization destroys all data on the token.

Note: On the other hand, until you put SafeNet PCIe HSM into service with actual production data, keys, and certificates on it, you can reinitialize it and practice with a variety of optional settings, as many times as you wish.

Many applications from PKI and other cryptographic product vendors do not include the capability to initialize a SafeNet HSM, so SafeNet supplies the Lunacm utility program on all supported platforms, to perform that function and other maintenance functions.

Your SafeNet PCIe HSM Cryptographic Module or HSM is shipped in a pre-initialized state, as part of the factory quality assurance process. However, in that state the HSM is not associated with Security Officer [SO] or User Authentication Data, and is not ready to receive or to create and store objects. You must perform a one-time initialization procedure with the lunacm utility before the HSM can operate with an application program.

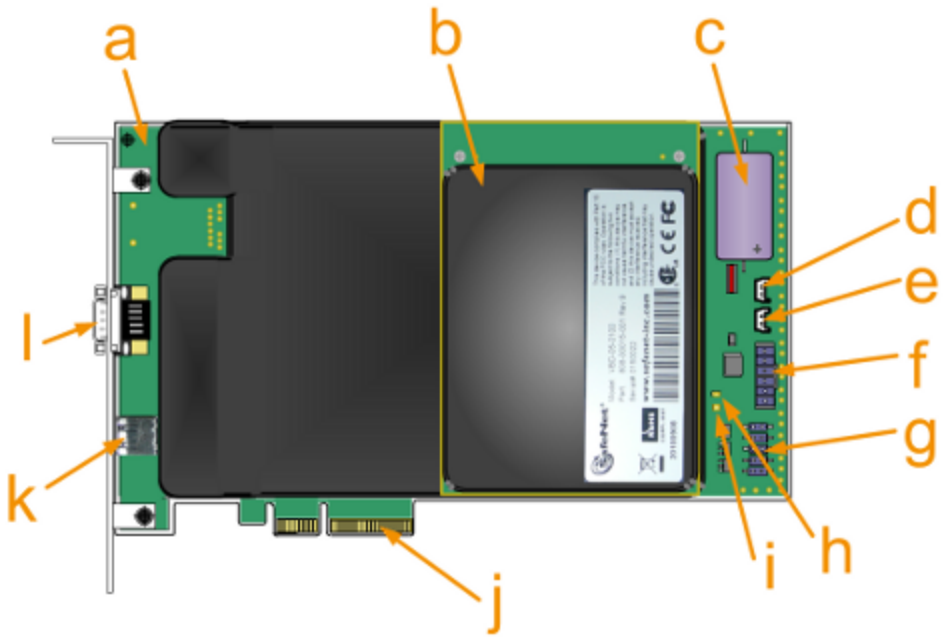
Sessions and Authentication

When you access a SafeNet HSM or HSM Partition, by providing the passwords (Password Authentication versions) or the PED Keys (Trusted Path Authentication versions), you open a session. That session remains open until you (or your application) explicitly close it.

Removing power from a SafeNet HSM immediately closes all sessions and causes all volatile data to disappear.

Your application program might not be capable of logging into SafeNet PCIe HSM, on its own. If not, then the program expects to encounter the HSM already in a logged-in state. For SafeNet PCIe HSM to operate with such an application, you must log into the token with the lunacm utility. Find it in your LunaPCI directory, following installation. Every time you reboot your computer, you are required to log into the HSM with the lunacm utility before you can resume using SafeNet PCIe HSM with your application, unless you have invoked Autoactivation.

SafeNet PCIe HSM Physical Appearance and Features



Feature	Description
a	K6 main board
b	Daughter board
c	Battery for Real Time Clock (RTC) and NVRAM
d	Header for Tamper2 (indicated as JP3 on the board), or the "decommission" circuit - closing/shunting those pins causes the KEK and any cached data to be erased. [If used, this is intended to be wired to a normally-open switch, accessible outside the host computer. Such a switch should be shielded/shrouded to prevent accidental activation. To ship the SafeNet PCIe HSM 6.x HSM to SafeNet (or other recipient) with assurance that your crypto objects cannot be recovered by anyone, just shunt this header momentarily, or touch a screw-driver blade to both pins simultaneously - the "decommission" action occurs instantly.]

Feature	Description
e	Header for Tamper1 (indicated as JP2 on the board), the physical tamper circuit - closing/shunting those pins, or closing a connected switch causes a tamper event and destroys the MTK, the Master Tamper Key that encrypts everything on the HSM. [If used, this pin pair would usually be wired to a chassis switch that is held open when the lid or panel is in place. Opening the lid or panel would close the switch and tamper the HSM.]
f	Serial Connector - not for customer use
g	PED port - same as the externally available PED port "m", below
h	Indicator LED D1 [ERROR] - glows red when the HSM is in an error state or system HALT [when the HSM senses a tamper of any type, or upon start-up if the HSM cannot initialize the dual-port communication between itself and the host computer]
i	Indicator LED D2 [ACTIVE] - glows or flickers green when the HSM is active
j	PCIe x4 card-edge connector - can be inserted in any PCIe 4-channel (or larger) socket
k	USB connector (for connection to backup HSM or a SafeNet DOCK 2 reader - appears as "Tunnel Slot" in LunaCM slot listing)
l	PED Port - connect a SafeNet SafeNet PED 2 PIN Entry Device, reads and imprints iKey PED Keys (a "something you have" authentication factor) that carry primary authentication for the HSM and HSM partitions; also provides a keypad interface for PED Key operation and for additional, optional "something you know" authentication factor], Use a SafeNet-supplied PED cable

Developing a security plan and associated procedures

Not every application environment will require rigorous security and paper-trail management, with respect to HSMs and their contents. However, in high-security environments where security and process auditing is mandated, you might be required to refer to a history of any sensitive materials and any systems associated with them -- who had access, what did they do, and when did they do it. Rehearse everyday operational activities, as well as maintenance and update activities (Authentication Data [password] update cycles, personnel changes, backups, logging) before implementation in your live environment.

Have all secure physical storage sites and all the related handling procedures prepared in advance. Log your receipt of the SafeNet hardware and then log all storage and handling events thereafter. In an operational environment, you should be able to refer back to a complete “paper trail” – an unbroken record that tracks the existence, storage, handling, and all transitions/hand-offs experienced by each token/HSM that you ever use. Once you take possession, never allow yourself or your organization to lose track, even briefly, of any of your HSMs. If your environment includes auditing, your security auditors will require such a record.

About SafeNet USB HSM

Your SafeNet USB HSM Cryptographic Module or HSM is shipped in a pre-initialized state, as part of the factory quality assurance process. However, in that state the HSM is not associated with Security Officer [SO] or User Authentication Data, and is not ready to receive or to create and store objects. You must perform a one-time initialization procedure with the `lunacm` utility before the HSM can operate with an application program.

Note: Initialization is meant to be performed only once on an HSM, and it erases any Authentication Data, data or token objects contained on the HSM. Once the HSM is in use, be sure to avoid mistakenly initializing it again. On the other hand, until you put the SafeNet USB HSM into service with actual production data, keys and certificates on it, you can reinitialize it and practice with a variety of optional settings, as many times as you wish.

Sessions and Authentication

When you access a SafeNet HSM or HSM Partition, by providing the passwords (Password Authentication versions) or the PED Keys (PED Authentication versions), you open a session. That session remains open until you (or your application) explicitly close it.

Removing power from a SafeNet HSM immediately closes all sessions and causes all volatile data to disappear.

Your application program might not be capable of logging into the SafeNet USB HSM, on its own. If not, then the program expects to encounter the HSM already in a logged-in state. For the SafeNet USB HSM to operate with such an application, you must log into the HSM or its User partition (sometimes referred to as a "token" in some cryptography documentation and discussions) using the `lunacm` utility. Find it in your SafeNet HSM Client directory, following installation. Every time you reboot your computer, you are required to log into the HSM with the `lunacm` utility before you can resume using the SafeNet USB HSM with your application, unless the application is SafeNet HSM-aware.

SafeNet USB HSM as Encryption/Signing HSM or as RA HSM

The SafeNet USB HSM is shipped in different configurations. The Password Authenticated version can be factory configured as an Encryption and Signature HSM (token) or as a Registration Authority (RA) HSM. An RA HSM has the same capabilities as an Encryption and Signature HSM, with the additional ability to wrap private keys off the token for use by smart cards and other applications where multiple secure key generation and issuance is required.

Develop a security plan and associated procedures

Not every application environment will require rigorous security and paper-trail management, with respect to HSMs and their contents. However, in high-security environments where security and process auditing is mandated, you may be required to refer to a history of any sensitive materials and any systems associated with them -- who had access, what did they do, and when. Rehearse everyday operational activities, as well as maintenance and update activities (Authentication Data [password] update cycles, personnel changes, backups, logging) before implementation in your live environment.

Have all secure physical storage sites and all the related handling procedures prepared in advance. Log your receipt of the SafeNet hardware and then log all storage and handling events thereafter. In an operational environment, you should be able to refer back to a complete “paper trail” – an unbroken record that tracks the existence, storage, handling, and all transitions/hand-offs experienced by each HSM that you ever use. Once you take possession, never allow yourself or your organization to lose track, even briefly, of any of your HSMs or authentication devices (PED Keys, for PED-authenticated HSMs).

If you don't know where a PED Key is, you are not in control of it. If you don't know where it has been, you cannot assert that it has not been copied. If this is ever in doubt, consider resetting or changing passwords/PED Keys. Partition authentication (password, black PED Key if applicable) can be reset with resetPw. Partition or HSM authentication can be changed with changePw. Consider exercising these options if there is any chance an HSM's authentication might have been compromised.

Password integrity is as secure as your personnel choose to keep those passwords.

Physical authentication devices (PED Keys) are as secure as your security policies and procedures and their enforcement.

About SafeNet Backup HSM

The SafeNet Backup HSM is physically similar to the SafeNet USB HSM, but is used exclusively to securely backup sensitive material from SafeNet HSMs, and to restore backed-up material to SafeNet HSMs. Some important characteristics are:

- The SafeNet Backup HSM can be connected locally, by USB cable, to the primary HSM, or it can be connected to a server and used to backup from, and restore to, remotely located primary HSMs.
- The SafeNet 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 (sometimes called the FIPS 140-2 level 2 version) when backing up a Password-authenticated primary HSM, and the same SafeNet Backup HSM becomes a PED-authenticated Backup HSM (sometimes called the FIPS 140-2 level 3 version) when backing up a PED-authenticated primary HSM.
- The SafeNet Backup HSM performs backup and restore operations only; it is not capable of cryptographic operations, and cannot (for example) be substituted for a SafeNet USB HSM.

Note: When the SafeNet Backup HSM contains backup data, and has therefore taken on the authentication characteristics of either a Password-authenticated or a PED authenticated HSM, it cannot restore to the other type. This is a security feature. PED-authenticated-to-Password-authenticated is prevented, because keys and objects that were created on a PED-authenticated HSM are more secure, and moving them to a less-secure type of HSM would be considered a breach of security. Password-authenticated-to-PED-authenticated is prevented because anyone seeing keys and objects on a PED-authenticated HSM is entitled to assume that those keys and objects have always had that level of security throughout their existence.

2
SafeNet HSM Authentication Types

This chapter describes the types of authentication available on SafeNet HSMs. Each SafeNet 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. See the following sections for more information:

- "About Password Authentication" below.
- "About PED Authentication" on page 30.
- "Comparing Password and PED Authentication" on page 33
- "About Remote PED" on page 35

Note: ***Authentication differences - Password-authenticated vs PED-authenticated***:

- 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, while
-- 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) - that is, there are two levels of protection, one administrative, and the other operational, where the operational level is gated by the administrative level.

- When the HSM is Password-authenticated,
-- the *administrative role secret is also the application-authentication secret*, one plain-text secret used for two purposes; the application that knows that secret declares the application partition open-for-business while in the act of accessing it with that single secret as its authentication - a single level of protection that is both administrative and operational. 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.

About Password Authentication

This section applies to versions of SafeNet HSM that control access via typed text-string authentication, or passwords, at all authentication levels. For SafeNet HSMs, this is sometimes referred to as "FIPS 140-2 Level 2" or simply "FIPS

Level 2" or "FIPS 2" authentication.

If you received a SafeNet PED and PED Keys, then your SafeNet appliance's HSM probably uses Trusted Path Authentication, and **not Password Authentication** (verify with the `hsm displayLicenses` command), and this page does not apply to you. We also can refer to that version as "FIPS 140-2 Level 3" authentication. See "About Trusted Path Authentication", instead.

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 Network HSM API to perform cryptographic functions within pre-assigned virtual HSMs (called Partitions) on the SafeNet system.

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

Role	Description
Appliance Admin	When you login to the SafeNet appliance via **lunash** the only accepted ID is "admin" which requires the admin password. As the appliance admin, you can connect and login locally, via a serial terminal, or remotely via SSH. With no other authentication, admin can perform general, appliance-level administration.
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 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**.

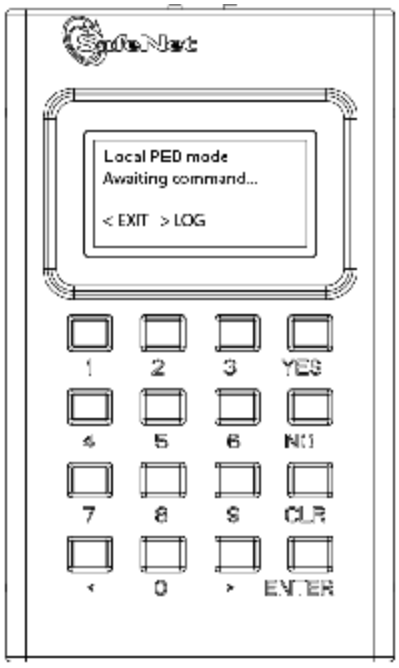
Summary

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.

About PED Authentication



This section applies to versions of SafeNet HSM that control access via Trusted Path Authentication - that is, HSMs that control access by means of the PED and PED Keys, rather than by typed-in text strings. For SafeNet HSMs, this is sometimes referred to as "FIPS 140-2 Level 3" or simply "FIPS Level 3" or "FIPS 3" authentication.

If you did not receive a SafeNet PED and PED Keys, then your SafeNet HSM probably uses Password Authentication, and not Trusted Path Authentication (verify with the **hsm displayLicenses** command), and the pages in this section do not apply to you. See "About Password Authentication" on page 28, instead.

You can also verify the type of a SafeNet HSM by running the **hsm showPolicies** command. The output includes these lines near the top:

```
Description                         Value
===========                         =====
Enable PIN-based authentication     Disallowed
Enable PED-based authentication     Allowed
```

The above result is from a PED-authenticated HSM. A Password-authenticated HSM would show:

```
Description                         Value
===========                         =====
Enable PIN-based authentication     Allowed
Enable PED-based authentication     Disallowed
```

PED Connections

The Trusted Path is the connection between the SafeNet PED and the SafeNet HSM.

- For SafeNet Network HSM, the PED connection is on the appliance front panel.
- For SafeNet 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 SafeNet USB HSM, the PED connection is an external connection to the device (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 connection is a cryptographically secured link across the network - when credentials travel between PED and HSM, they are encrypted throughout the journey. 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 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 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.

Roles

For SafeNet HSM with Trusted Path Authentication, the various layered roles are protected by a combination of PED Keys and passwords:

Appliance Admin (SafeNet Network HSM only)

When you login to the SafeNet appliance via lunash the accepted IDs are "admin" which requires the admin password, "operator", which requires the operator password, or "monitor" which requires the monitor password. (Named users can later be added with admin, operator, or monitor authority.) The password is typed at the command line (operator and monitor are restricted identities that have access to subsets of the lunash command set used by admin).

As the appliance admin, you can connect and log in locally, via a serial terminal, or remotely via SSH. With no further authentication, admin can perform general, appliance-level administration (not accessing the HSM), and can run view/list/show/display commands on the HSM that do not make changes.

Admin sees the full available command set, while operator- and monitor-level users see only subsets.

If any administrative user attempts an HSM command that needs authentication, the interface prompts for that authentication. On PED-authenticated systems, you are directed to the PED, which prompts for PED Keys and keypad actions.

EXCEPTION: You can also log in through the local (serial link) console connection as an identity called "recover" (password "PASSWORD").

HSM Admin or 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 or HSM Admin (of which there can be only one per SafeNet HSM).

The authentication data for SO/HSM Admin is not a password. It 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 SafeNet PED, or at the configured Remote SafeNet PED, to insert the required blue PED Key, when prompted. Otherwise, HSM commands cannot be used.

Thus, anyone wishing to issue HSM-wide administrative commands to the SafeNet appliance must be present in the room with the SafeNet PED, and must have the cooperation of the SO/HSM Admin blue PED Key holder (who, in turn, needs physical access to the connected SafeNet PED).

The options are to perform such authentication via a PED connected physically to the HSM appliance, or to perform authentication via a PED connecting through a secured Remote PED connection.

Partition User or (Crypto Officer)

To access HSM Partitions to perform Partition-specific administration tasks, such as

- set Partition-specific policies
- assign Partition to Clients
- revoke Clients, etc.

You must be authenticated as Partition User (of which there can be one per HSM on SafeNet PCIe HSM or SafeNet USB HSM, or there can be several on SafeNet Network HSM -- one for each Partition in the HSM), and for that you use the Partition User black PED Key.

The authentication data for Partition User (also known as Crypto Officer in some security and authentication schemes) is both a password and a secret carried on a black PED Key. As the Partition User/Crypto Officer, you can connect locally, via a serial terminal, or remotely via SSH. To perform Partition administration on SafeNet Network HSM, you must first be logged in as admin to have access to **lunash** commands.

For SafeNet PCIe HSM and SafeNet USB HSM, you simply need access to the host computer, where you can use **lunacm** commands. For the Partition User/Crypto Officer to login and issue Partition administration commands, someone must be present at the connected SafeNet 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. Otherwise, Partition administration commands cannot be used.

If you have invoked the Crypto Officer/Crypto User distinction, then there are two Partition Passwords, but only the Crypto Officer password allows you to run **lunash** or **lunacm** commands to administer the Partition. The Crypto User password allows only a limited set of cryptographic activities via a Client application.

For SafeNet Network HSM, good security practices suggest that the Partition Password should be different than the appliance admin password and different than other Partition Passwords (for other Partitions). If Crypto Officer/Crypto User are in force, then their passwords should differ as well. However, your corporate policies might vary.

Client (or Crypto User)

To access HSM Partitions with an application to perform cryptographic operations on data, (for SafeNet Network HSM only, requires that you connect remotely via SSL as a Client that has been registered by certificate exchange and assigned by the Partition User to this Partition), 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).

At this point, the two models diverge:

- 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 SafeNet 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 (for SafeNet Network HSM) that gives access to `lunash` command line. For SafeNet PCIe HSM and SafeNet USB HSM, the

password or other authentication that gives access the client application (that uses the HSM for crypto operations) 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.

Summary

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.

Audit

Not mentioned above is the 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. These roles are distinct and separate from other roles on the appliance and the HSM, conforming to the requirements of auditing standards.

Using SafeNet PED Remotely

By default, SafeNet PED is connected locally, and powered by the HSM using one cable. However, SafeNet PED can also be used remotely from the HSM or HSMs for which it manages access control. See "About Remote PED" on page 35.

Comparing Password and PED Authentication

The following table outlines the key differences between PED and password authentication.

Feature	Password-authenticated HSM	PED-authenticated HSM
Ability to restrict access to cryptographic keys	• knowledge of Partition Password is sufficient • for backup/restore, knowledge of partition domain password is sufficient	• ownership/possession of the black PED Key is mandatory to modify keys, gray PED Key to use without modifying • for backup/restore, possession of both black and red PED Keys is necessary • the Crypto User role is available to restrict access to usage of keys, with no key management • option to associate a PED PIN (something-you-know) with any PED Key (something you have), imposing a two-factor authentication requirement on any role
Dual or Multi-person Access Control	• not available	• Mof N (split-knowledge secret sharing) requires "M" different holders of portions of the role secret, in order to authenticate to an HSM role - can be applied to any, all, or none of the administrative and management operations required on the HSM

Feature	Password-authenticated HSM	PED-authenticated HSM
		• prevents unilateral action by a single actor
Key-custodian responsibility	• linked to password knowledge, only	• linked to partition password knowledge, • linked to black PED Key(s) ownership
	Roles limited to: • Appliance admin (SafeNet Network HSM only) • HSM Admin (SO) • Partition SO • Partition Crypto Officer • Partition Crypto User	Available roles: • Appliance admin • HSM Admin (Security Officer) • Domain (Cloning / Token-Backup) • Secure Recovery • Remote PED • Partition Owner (or Crypto Officer) • Crypto User (usage of keys only, no key management) for all roles, two-factor authentication (selectable option) and MofN (selectable option)
Two-factor authentication	• not available	• physical PED Key per role • optional to impose requirement for PED PIN (multi-digit code input at PED keypad), different for each role, can also be different for each legitimate copy of a PED Key
Two-factor authentication for remote access	• not available	• Remote PED and orange (Remote PED Vector) PED Key deliver highly secure remote management of HSM, including remote backup
Location	Authentication can be input locally, or from a remote terminal (RDP, SSH, etc.)	Authentication requires local physical connection, or pre-configured Remote PED link
Security and Handling Advantage	• Easy/quick to change if/when necessary (for personnel change, suspected compromise, etc.). • Can comply with an organization's password-aging policy without hardship.	• No written record of a complicated password, that might be compromised. • Access and handling of physical devices (PED Keys) can be tracked and controlled (who has, when used, etc.). • Duplication and promulgation can be prevented by physical security measures. • If PED PIN option is used, easy to block view of PED keypad input from bystanders or cameras. • If PED PIN option is used, no exposure of PED PINs outside the PED (does not exist on a bus, is not sent over any communication channel).
Security and Handling Disadvantage	Password vulnerable to • watchers (or cameras) observing password being typed)	• Requires hands-on, physical action by personnel to perform changes of authentication secrets (in case of compromise or in conformance with organizational policy). • Scheduled/mandated "password-change" cycles in an

Feature	Password-authenticated HSM	PED-authenticated HSM
	mal-ware (keystroke loggers, etc.) • secure PWs are obscure and must be written; record must be securely stored • difficult to know who might have seen or been told a password	organization can be logistically intensive when HSMs share PED Key secrets.
Separation of roles	Not possible to enforce unless secret holders are never allowed to meet or communicate.	Physical and procedural control of physical PED Keys and their handling enforces separation of roles.

About Remote PED

When it is not convenient to be physically near the host computer that contains a SafeNet HSM, in order to connect a SafeNet PED and present required PED Keys, you can operate remotely and securely.

The PED-Authenticated SafeNet 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 interaction can then be accomplished with SafeNet PED and PED Keys that are physically distant from the HSM, as follows:

- One computer, running a supported OS, hosts the HSM - this could be:
  - a server or tower containing a SafeNet PCIe HSM, or
  - a server or other computer with a USB-connected SafeNet USB HSM, or
  - a SafeNet 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
- A second computer (laptop, workstation, server running a supported Windows version) has a SafeNet 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 and purple, as well) PED Keys that were imprinted with the HSM previously,
  - or blank blue, black. and red (optionally, white and purple) PED Keys that are about to be imprinted along with the HSM.
- The HSM is told to look to a remote PED for its authentication requests.
- The PED host computer has the LunaPED driver installed, and runs the pedserver utility.

- The HSM host computer runs the pedclient utility, and the HSM is told to connect to the Remote PED.
- 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) agree that the provided orange PED Key contains the same Remote PED Vector as is imprinted on the HSM, and the secure Remote PED link is established.
- 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..

3
Configurations

This document discusses configurations in two ways:

- combinations of capabilities and characteristics that are mostly pre-determined by the model you order from the factory
- combinations of settings and options that you can modify to suit your situation and needs after receiving your HSM

The factory-built configurations, along with some notes about their interactions and exclusions are discussed at:

- "Factory-Installed HSM Configurations" below

In addition to factory-built configurations, you can also update to newer firmware versions, or purchase and apply certain enhancements after receiving your SafeNet HSM, in the form of Capability Upgrades, discussed at:

- "Firmware Updates and Capability Upgrades" on page 40

The remainder of this chapter introduces some after-purchase configurations that you can perform with your SafeNet HSM products, including some that are mandatory in order to make use of your SafeNet HSM, and some that are optional (and might, or might not, require additional equipment or software) that can enhance the utility and usability of your SafeNet HSMs. The various configurations are introduced in the following sections:

- "High Availability (HA) Configurations" on page 41
- "Backup and Restore Configurations" on page 48
- "Host Trust Link (HTL) Configurations" on page 49

Factory-Installed HSM Configurations

SafeNet HSMs ship from the factory in various configurations that provide different levels of authentication, performance, and key management capabilities, as detailed below. These options are selected at the time of purchase and cannot be modified. A table listing the available or supported SafeNet HSM models is provided at the end of this section.

Authentication Variants

You can purchase either a password-authenticated (FIPS 140-2 Level 2) HSM or a PED-authenticated (FIPS Level 3) HSM.

Password Authentication

Password-authenticated HSMs provide single-factor authentication for all roles, using passwords. SafeNet HSMs enforce the use of strong passwords by requiring the passwords to conform to the following rules:

- minimum length of eight characters
- must include characters from at least three of the following character classes:
  - lowercase alphabetic (abcd...xyz)

- uppercase alphabetic (ABCD…XYZ). If used as the first character in the password, does not count towards the number of character classes used.
- numeric (0123456789). If used as the last character in the password, does not count towards the number of character classes used.
- special (non-alphanumeric, -_!@#$%&*…)

SafeNet password-authenticated HSMs are validated to FIPS 140-2 Level 2. See "About Password Authentication" on page 28 for more information.

PED Authentication

PED-authenticated HSMs provide two-factor or multi-factor authentication for all roles, using a PED, PED Keys, and PINs. A PED is a physical device, equipped with a numerical keypad, that is securely connected to the HSM, either locally or remotely (see "About the SafeNet PED" on page 1). To authenticate to a PED-authenticated HSM, you require a PED Key, which is an iKey USB token, physically similar to a thumb drive. Separate PED keys are required for each role, and each role supports multi-factor authentication, which can include:

- something you have (the physical PED Key, see "About PED Keys" on page 1)
- something you know (a PED PIN, optionally associated with a PED Key, entered at the PED keypad; see "What is a PED PIN?" on page 1)
- a further option of MofN secret splitting, per role (see "About MofN" on page 64)

MofN is optional split-knowledge, shared-secret access control, where the access secret for a role is split among quantity **N** PED Keys, with quantity **M** of those PED Keys required for authentication. That is, each key in an MofN context is a portion of the full role secret, and not the complete secret, thus preventing any single PED Key holder gaining unsupervised access to that role on the HSM.

SafeNet PED-authenticated HSMs are validated to FIPS 140-2 Level 3. See "About PED Authentication" on page 30 for more information.

Key Management Variants

SafeNet HSMs store all key material in hardware. Depending on your security requirements and key management practices, you may need to move or copy key material from the HSM to a backup HSM, another HSM in the same HA group, or to a file for off-board storage or use. To support these different key management scenarios, SafeNet HSMs are available in the following key management configurations. The variants are mutually exclusive - only one variant can apply to an HSM.

> **Note:** The ordering code for each key management variant is indicated in parentheses, if applicable.

Cloning (CL)

A SafeNet HSM with cloning (CL) provides the following key management capabilities:

- All keys/objects can be cloned to other SafeNet HSMs, or to a SafeNet Backup HSM.
- All keys/objects are replicated when configured in an HA group.
- Private keys cannot be wrapped off the HSM (that is, you cannot export private keys to an encrypted file).

Note: You can clone keys/objects only between HSMs or HSM partitions that share the same cloning domain.

In the cloning configuration, the RSA private key is normally static and would reside throughout its lifetime within the HSM, for a root-key application.

Cloning With Key Export (CKE)

A SafeNet HSM with cloning with key export (CKE) provides the following key management capabilities:

- All keys/objects, except private keys, can be cloned to other SafeNet HSMs or to a SafeNet Backup HSM.
- All keys/objects, except private keys, are replicated when configured in an HA group.
- Private keys can be wrapped off the HSM (that is, you can export private keys to an encrypted file).

CKE is normally used for smart card and identity issuance, where transient RSA key-pairs are generated, wrapped off, and issued to a user. They are not used on the HSM. They are simply generated securely, then deleted from the HSM after wrapping off.

No Backup

A SafeNet HSM with no backup provides the following key management capabilities:

- Keys/objects cannot be cloned to other SafeNet HSMs or to a SafeNet Backup HSM.
- Private keys cannot be wrapped off the HSM (that is, you cannot export private keys to an encrypted file).

An HSM without backup capability ensures that created/contained keys can never leave the HSM. This configuration might also be used when keys are intended to have short lifespans, and would not be expensive to replace.

Performance Variants

The SafeNet Network HSM and SafeNet PCIe HSMs are available in low performance (1700 signings/second) or high performance (7000 signings/second) variants. The SafeNet USB HSM is available in a single performance level.

SafeNet HSM Models

The following table provides a listing of the available or supported SafeNet HSM models.

Table 1: SafeNet HSM models

Model	Performance	Authentication	CL	CKE	No Backup
SafeNet Network HSM	1700	Password	X	X	
		PED	X	X	X
	7000	Password	X		
		PED	X		X

Model	Performance	Authentication	CL	CKE	No Backup
SafeNet PCIe HSM	1700	Password	X	X	
		PED	X	X	
	7000	Password	X		
		PED	X		
SafeNet USB HSM		Password	X	X	X
		PED	X	X	

Firmware Updates and Capability Upgrades

This section discusses installable modifications that many customers would make before placing their SafeNet HSM into service.

Firmware Updates

The HSM firmware determines the operation and features of the HSM. Newer firmware versions are constantly in development, to implement fixes, to add new functionality, or to adapt to evolving standards and certifications. As firmware versions are tested and released, they are made available to SafeNet customers. However, the newest version is rarely the version that is installed at the factory.

The United States National Institute of Standards and Technology's FIPS (Federal Information Processing Standard) 140-2 is a widely respected standard in the cryptographic industry. Many customers are required by their industry or market or auditing agency to use only FIPS-validated HSMs. SafeNet HSMs are routinely submitted to validation laboratories to be validated against the standard. For an HSM that has previously been validated, new submissions are made for re-validation when the device firmware has substantially changed.

New SafeNet HSMs are shipped from the factory with the most recent FIPS-validated firmware version installed. This is for the benefit of customers who are required to use only FIPS-validated HSMs in their operations. Because validation updates can take a year or more, there are always versions of firmware newer than the validated version. The newest, for the current release, is shipped with the HSM, ready to install, or can be downloaded from SafeNet, if the customer wishes to apply the latest fixes and features, and is not constrained to use only FIPS-validated HSMs.

The latest (at the time) firmware might also be an in-progress validation candidate, and so is ready for FIPS-requiring customers to install, as soon as the updated validation certificate is released.

Updating the HSM firmware is as simple as:

- having the Firmware Update File in place on the host,
- logging into the HSM, and
- issuing an update command (with an authentication code that you received from SafeNet).

Firmware updates can be reversed by a rollback command that returns the HSM to the previously-installed version. You might, for example, choose to perform firmware rollback in a test laboratory after evaluating the newer firmware for your needs.

Capability Upgrades

Capability upgrades are additional sets of optional enhancements that can be purchased and applied to SafeNet HSMs. For example, a capability upgrade might add cryptographic algorithms/mechanisms that were not part of the base HSM, or might add the ability to use small form-factor backup devices.

The process is similar to a firmware update:

- acquiring the capability upgrade package from SafeNet,
- placing it on the host computer with the HSM
- logging into the HSM
- running an update command (with an authentication code that you received from SafeNet).

High Availability (HA) Configurations

SafeNet HSM products include availability and scalability capabilities for mission critical applications that require uninterrupted up-time. These features allow the grouping of multiple devices into a single logical group – known as an HA (High Availability) group. 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 linear performance gains for many applications. The following sections describe these features and the available configuration options in detail to help you understand how best to configure the HA groups for their application and environment.

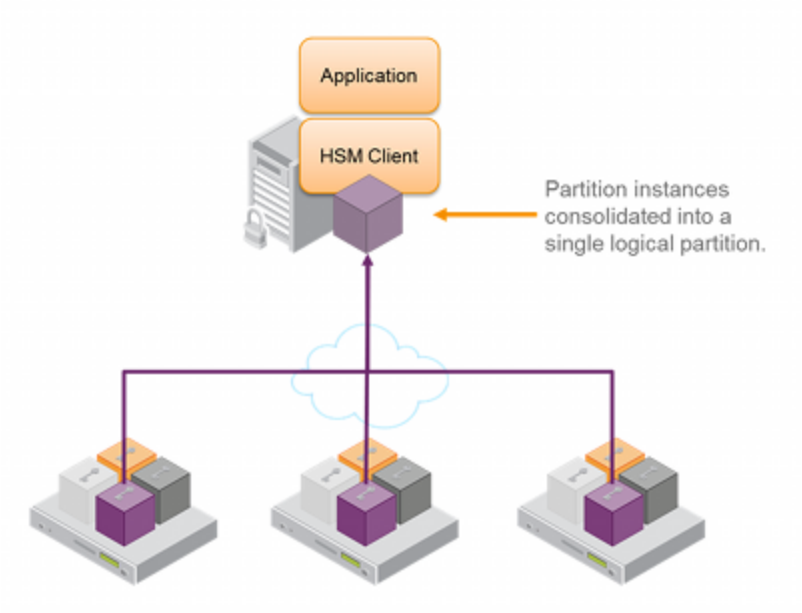
Overview

The SafeNet high-availability (HA) and load balancing (LB) functionality is implemented in the HSM client libraries, and uses the SafeNet cloning[1] function to replicate/synchronize content across HA-group members. The HSMs and appliances are not involved and, except for being instructed to clone objects to certain HSMs during a synchronization operation, are unaware that they might be configured in an HA group. This allows you to configure HA on a per-application basis. On each application server, define an HA group by first registering the server as normal clients to all the desired HSMs, then use client-side administration commands to define the HA group and set any desired configuration options. You can configure several options including:

- setting automatic or manual recovery mode;
- setting some HSMs as standby members; and
- performing various manual synchronization and recovery operations.

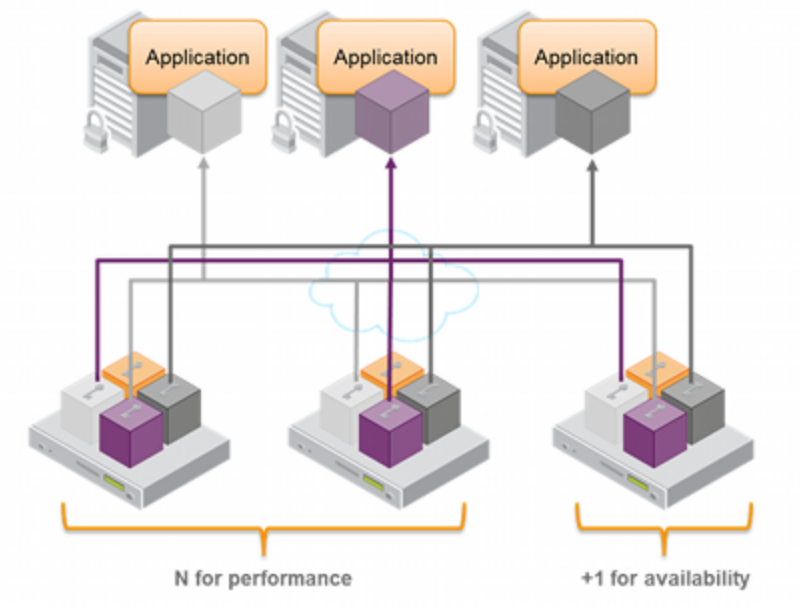
Once defined, the library presents to the application a virtual HSM that is a consolidation of all the physical HSMs in the HA group. From this point on the library distributes operations and automatically synchronizes key material transparently to the application.

[1]The duplication or copying of HSM or application partition contents to other HSMs or application partitions that share the cloning domain secret. Cloning copies objects (certificates, keys, data), in a secure manner, via trusted path, from the user space on one HSM to an equivalent space on a second HSM. The trusted path can be direct connection between HSMs or application partitions on the same host, or can be via Remote Backup Protocol (RBC) between distant HSMs.

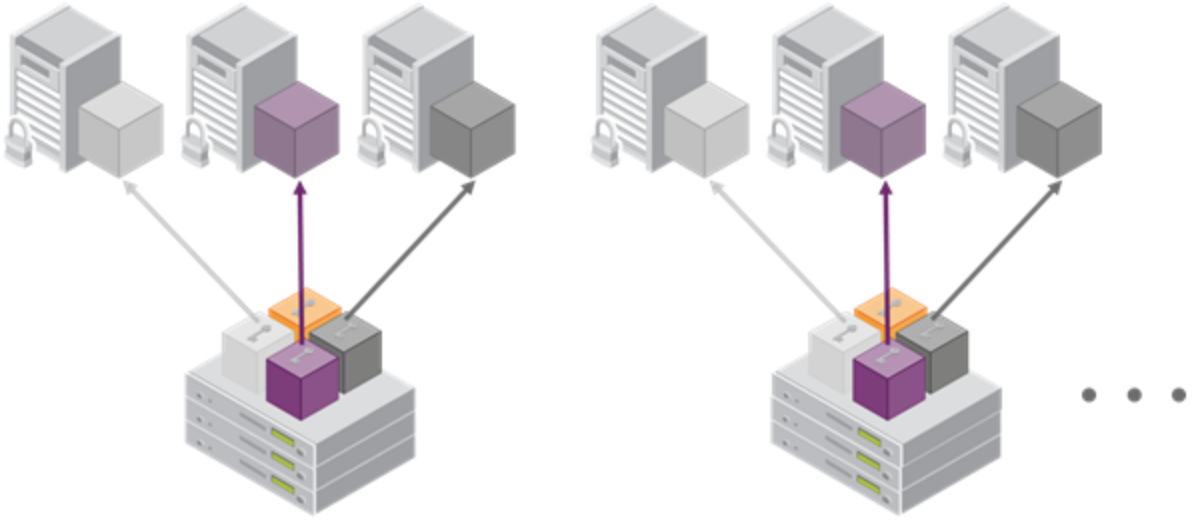


High Availability

As of SafeNet 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. A common practice is to set the group size to N+1 where N is defined by the desired performance per application server(s). As depicted below, this solution gives the desired performance with a single extra HSM providing the availability requirement. The number of HSMs per group of application servers varies based on the application use case but, as depicted, groups of three are typical.



As performance needs grow beyond the performance capacity of three HSMs, it often makes sense to define a second independent 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.



For detailed discussion of the HA feature, its constraints and parameters, and how to configure and use HA, refer to the SafeNet HSM Administration Guide.

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 fail-over 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 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 – creating a round-robin behavior. 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 – creating a least-busy behavior. This modified round-robin has the advantage of biasing load away from any device currently performing a lengthy-command. In addition to this least-busy bias, the type of command also affects the scheduling algorithm.

Single-part (stateless) cryptographic operations are load-balanced. However, multi-part (stateful) and key management commands are not load-balanced. 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 either are not used or are infrequent actions, so most applications are not affected by this restriction. 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. That is 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 also an infrequent occurrence for most applications .

It is important to understand that the least-busy algorithm uses the number of commands outstanding on each device as the indication of its busyness. When an application performs a repeated command set, this method works very well. However, when the pattern is interrupted, the type of command can have an impact. For example, when the HSM is performing signing and an atypical asymmetric key generation request is issued, some number of the application's signing commands are scheduled on the same device (behind the key generation). Commands queued behind the key generation therefore have a large latency driven by the key generation. However, the least-busy characteristic automatically schedules more commands to other devices in the HA group, minimizing the impact of the key generation.

It is also important to note that the load-balancing algorithm operates independently in each application process. Multiple processes on the same client or on different clients do not share their "busyness" information while making their scheduling choice. In most cases this is reasonable, but some mixed use cases might cause certain applications to hog the HSMs.

Finally, 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.

In summary, the load-balancing scheme used by SafeNet is a combination of round-robin and least-busy for most operations. However, as required, the algorithm adapts to various conditions and use cases so it might not always emulate a round-robin approach.

Failover

When an HA group is running normally the client library continues to schedule commands across all members as described above. The client continuously monitors the health of each member at two different levels. First, the connectivity with the member is monitored at the networking layer. Disruption of the network connection invokes a fail-over event within a twenty second timeout . Second, every command sent to a device is continuously monitored for completion. Any command that fails to complete within twenty seconds also invokes a fail-over event. 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 fail-over events.

A fail-over 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. So 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 . Note that the least-busy scheduling algorithm automatically minimizes the number of commands that stall on a failing unit during the twenty second timeout.

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 operation are transparently restarted on a new group member. In the event that the primary unit fails, any in-progress, multi-part, cryptographic operations must be restarted by the application, as the operation returns an error code.

As long as one HA group member remains functional, cryptographic service is maintained to an application no matter how many other group members fail. As discussed in the Recovery section below, members can also be put back into service without restarting the application.

Recovery

After a failure, the recovery process is typically straight-forward. Depending on the deployment, an automated or manual recovery process might be appropriate. In either case there is no need to restart an application!

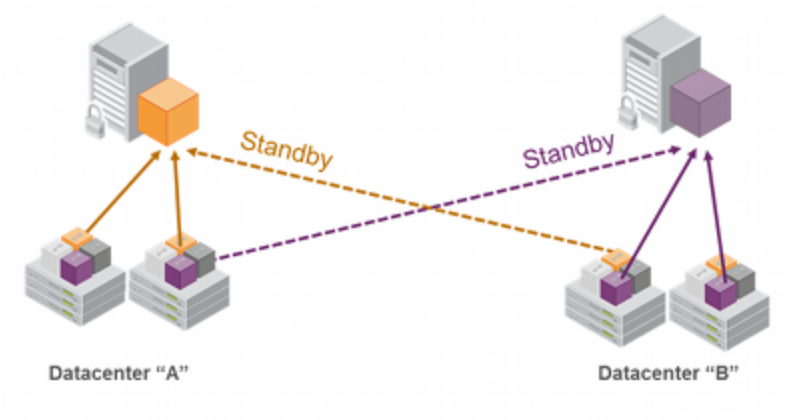
With automatic recovery, the client library automatically performs periodic recovery attempts while a member is failed. The frequency of these checks is adjustable and can be limited on the number of re-tries. Each time a reconnection is attempted, one application command experiences a slight delay while the library attempts to recovery. As such, the retry frequency cannot be set any faster than once per minute. Even if a manual recovery process is selected the application does not need to be restarted. 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 .

Sometimes a failure of a device is permanent. In this event, the only solution is to deploy a new member to the group. In this case, remove the failed unit from the HA group, add a new device to the group and then kick the recovery process. The running clients automatically resynchronize keys to the new member and start scheduling operations to it.

Finally, sometimes both an HSM and application fail at the same time. If, while an HSM was offline, no new key material was created the recovery is still straightforward: simply return the HSM to service and then restart the application. However, if new key material was created after an HSM failed but before the application failed, a manual re-synchronization might be required. Confirm which member or members have the current key material (normally the unit (s) that was online at the time the application failed). Put them back in service with the application. Then, for each member that has stale key material (a copy of an object that was deleted; or an old copy of an object who's attributes were changed), delete all their key material after first making sure they are not part of the HA group. Be particularly careful that the member is not part of the HA group or the action might destroy active key material by causing an accidental synchronization during the delete operation! After the HSM is cleared of key material, rejoin it to the group and the synchronization logic automatically repopulates the device's key material from the active units.

Standby Mode

By default all members in an HA group are treated as active. That is, they are both 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. Standby members are registered just like active members except, after they are added to the HA group, they are defined as "standby". As depicted below, applications can be deployed in geographically dispersed locations. In this scenario, use Luna's standby capability to use the HSMs in the remote data center to cost effectively improve availability. In this mode, only the local units (non-standby) are used for active load-balancing. However, as key material is created they are automatically replicated to both the active (local) units and standby (remote) unit. In the event of a failure of all local members the standby unit is automatically promoted to active status.. The primary reason for using this feature is to reduce costs while improving reliability and this approach allows remote HSMs that have high latency to be avoided when not needed. However, in the worst case scenario where all the local HSMs fail, the remote member automatically activates itself and keeps the application running.



Notes and More

It is important that all members in an HA group have the same configuration and version. Running HA groups with different versions is unsupported. Ensure that HSMs are configured identically to ensure smooth high availability and load balancing operation. SafeNet 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.

It is also critical that all members in an HA group share the same Security Domain role (Red PED key for Trusted Path authentication devices and security domain password for password authenticated devices). The Security Domain defines which HSMs are allowed to share key material. Because HA group members are, by definition, intended to be peers they need to be in the same Security Domain.

By default the client library present 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. As such, 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.

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).

The SafeNet HA and load-balancing feature works on a 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. This simplifies the configuration management associated with the HA feature.

When a client is configured to use automatic recovery the manual recovery commands must not be used. Invoking them can cause multiple concurrent recovery processes which result in error codes and possible key corruption .

Most customers should enable automatic recovery in all configurations. We anticipate that the only reason you might wish to choose manual recovery is if you do not want to impart the retry time to periodic transactions. That is, each time a recovery is attempted a single application thread experiences an increased latency while the library uses that thread to attempt the re-connection (the latency impact is a few hundred milliseconds).

Example: Database Encryption

This section walks through a specific sample use case of some of the HA logic with a specific application – namely a transparent database encryption.

Typical Database Encryption Key Architecture

Database engines typically use a two-layered key architecture. At the top layer is a master encryption key that is the root of data protection. Losing this key is equivalent to losing the database, so it obviously needs to be highly durable. At the second layer are table keys used to protect table-spaces and/or columns. These table keys are stored with the database as blobs encrypted by the master encryption key. This architecture maps to the following operations on the HSM:

1. Initial generation of master key for each database.
2. Generation and encryption of table keys with the master key.
3. Decryption of table keys when the database needs to access encrypted elements.
4. Generation of new master keys during a re-key and then re-encrypting all table keys with it.
5. Generation and encryption of new table keys for storage in the database (often done in a software module).

The HSM is not involved in the use of table keys. Instead it provides the strong protection of the MEK which is used to protect the table keys. Users must follow backup procedures to ensure their MEK is as durable as the database itself. Refer to the backup section of this manual for proper backup procedures.

HSM High Availability with Database Encryption

When the HSMs are configured as an HA group the database's master key is automatically and transparently replicated to all the members when the key is created; and each time it is re-keyed. If an HSM group member was offline or fails during the replication it does not immediately receive a copy of the key. Instead the HA group proceeds after replicating to all of the active members. Once a member is re-joined to the group the HSM client automatically replicates the new master keys to the recovered member.

With this in mind, before every re-key event the user should ensure the HA group has sufficient redundancy. A re-key will succeed so long as one HA group member exists, but proceeding with too few HSMs will result in an availability risk. For example, proceeding with only one HSM means the new master key will be at risk since it exists only on a single HSM. Even with sufficient redundancy, SafeNet recommends maintaining an offline backup of a database's master key.

HSM Load Balancing with Database Encryption

While a database is up and running the master key exists on all members in the HA group. As such, requests to encrypt or decrypt table keys are distributed across the entire group. So the load-balancing feature is able to deliver improved performance and scalability when the database requires a large number of accesses to the table keys. With that said, most deployments will not need much load-balancing as the typical database deployment results in a small number of table keys.

While the table keys are re-keyed, new keys are generated in the HSM and encrypted for storage in the database. Within an HA group, these keys are generated on the primary HSM and then, even though they exist on the HSM for only a moment, they are replicated to the entire HSM group as part of the availability logic. These events are infrequent enough that this extra replication has minimal impact.

Conclusion

The SafeNet high availability and load balancing features provide an excellent set of tools to scale applications and manage availability of cryptographic services without compromising the integrity of cryptographic keys. They do not need to be copied out of an HSM and stored in a file to achieve high levels of availability. Indeed, recovery from many failures is much more rapid with Luna's keys-in-hardware approach since each HSM maintains its own copy of all keys directly inside it. A broad range of deployment options are supported that allow solution architects to achieve the availability needed in a manner that optimizes the cost and performance without compromising the assurance of the solution.

Backup and Restore Configurations

While some applications might deal in ephemeral objects (keys, certs, other) that are erased after using, in many SafeNet 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.

For SafeNet Network HSM, the backup option is the SafeNet Remote Backup HSM, which can be connected directly to the SafeNet Network HSM to perform backup or restore operations on the spot. 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. The Backup HSM is not able to perform cryptographic operations; it functions only in its secure backup/restore role. The Backup HSM configures itself to be Password Authenticated or PED Authenticated, according to the HSM that it backs up. This is negotiated at backup time. See the Administration Guide for more detailed information and instructions.

For SafeNet PCIe HSM, the backup option is the SafeNet Remote Backup HSM, which can be connected directly to the SafeNet PCIe HSM to perform backup or restore operations on the spot. 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. The Backup HSM is not able to perform cryptographic operations; it functions only in its secure backup/restore role. The Backup HSM configures itself to be Password Authenticated or PED Authenticated, according to the HSM that it backs up. This is negotiated at backup time. See the Administration Guide for more detailed information and instructions.

For SafeNet USB HSM, the backup option is cloning of HSM or partition contents to another SafeNet USB HSM, which must be of the same authentication type (Password authenticated, or PED authenticated). See the Administration Guide for more detailed information and instructions.

Host Trust Link (HTL) Configurations

The traditional model had an application server acting as a client engaging an HSM server so that together they could provide secured application and crypto services to end-users. The application server (a computer in a server room, acting as a client to the HSM, and acting as a server to your users), the HSM server (in that same server room, or another, providing secure cryptographic services and/or acceleration for your client-server transactions), and the end-user consumer of services were all individual computers in the physical possession and control of their various owners.

That model is going away, replaced by scenarios where application servers can be Virtual Machine instances, rather than individual specific computers.

Virtualization brings a number of benefits. Among those, a virtual client is:

- flexible
- portable
- not tied to a specific hardware platform.

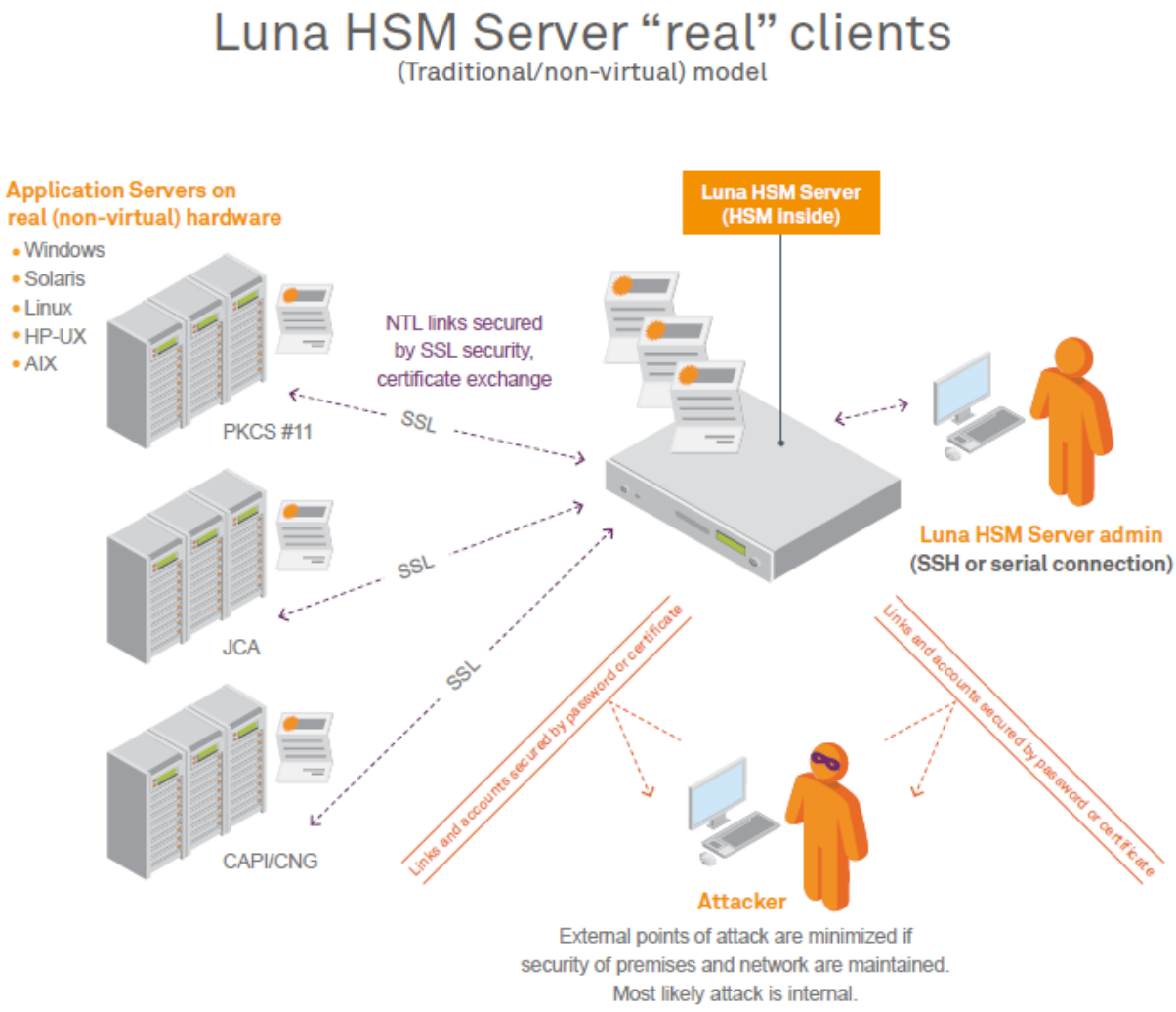
Virtual Machines are being deployed in:

- Private Cloud – an enterprise creates its own virtual-machine environment to serve the enterprise's constituent departments or business units; the private cloud remains invisible and inaccessible to outsiders
- Hybrid Cloud – an enterprise creates its own virtual-machine environment that it makes available for internal use and also provides as a service to its external customers
- Public Cloud – an enterprise creates a virtual-machine environment that it makes available as its primary service to businesses and individuals

Both the traditional and virtual-machine environments rely on HSMs and HSM servers to secure data and transactions, and accelerate the cryptographic aspects of transactions, as well as to secure important keys and certificates.

What Threats Come with Advances in Virtual Technology?

The threat of a stolen Server has always been a security concern for Enterprises. Traditionally this form of attack was relatively difficult, as walking out of a Data Center with a server should be rather difficult. Historically, the Enterprise supplied their primary data product, such as database or application access, supported by back-room cryptographic services from SafeNet HSMs. The Enterprise provided physical security for their application/database servers and for their SafeNet HSMs and HSM Servers, while SafeNet products provided the link security via the Network Trust Link (NTL) service. This threat paradigm shifted significantly with the introduction of virtualized server instances.



The threat has now evolved from traditional (steal the server) to virtual (steal the server Virtual Machine instance).

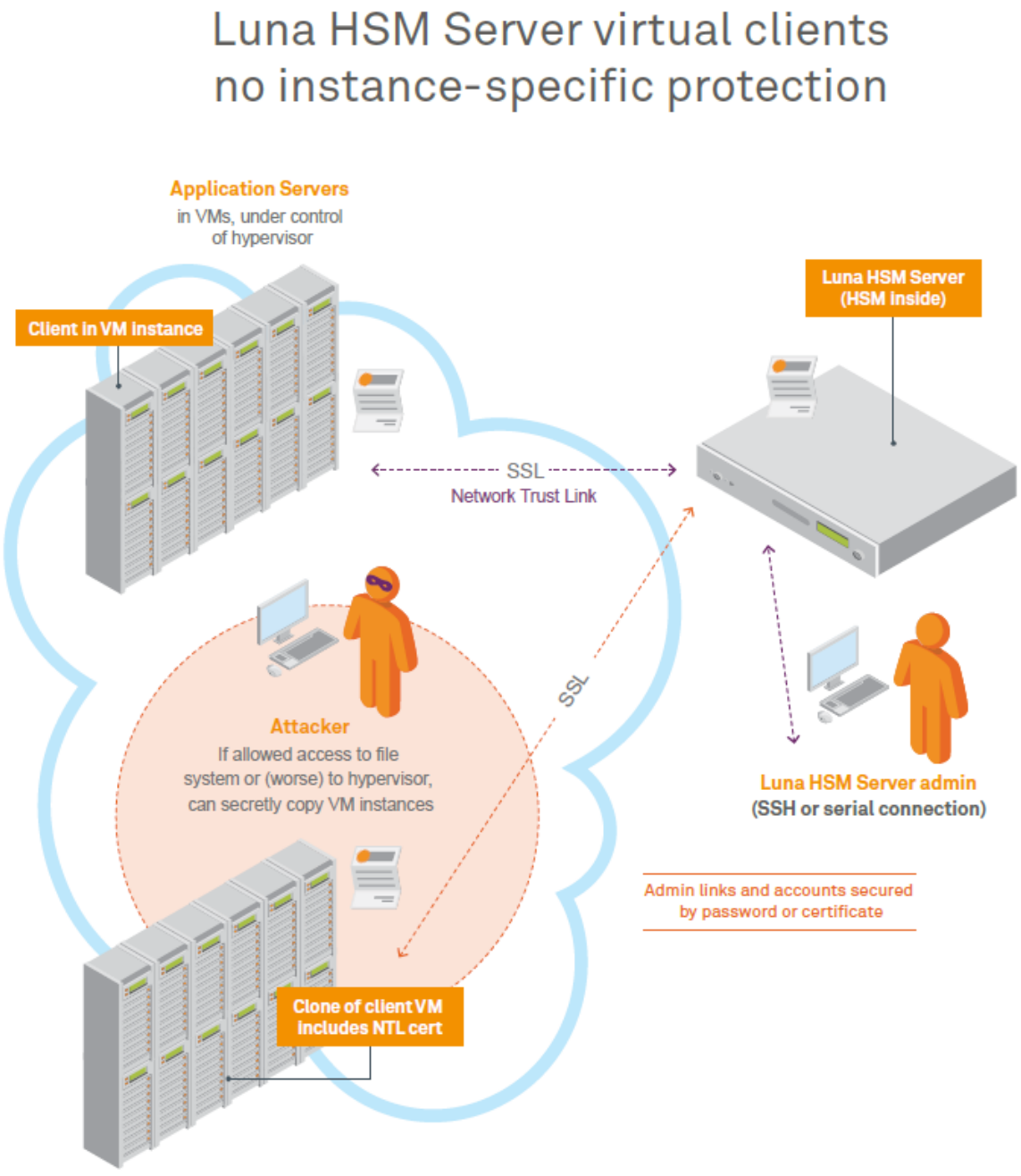
Virtual Clients

When the client employs the leverage of virtual hosting, that client could exist potentially anywhere in the world. The location could change at any time, unannounced. Importantly, multiple instances of a VM can be launched at any time, and control over the VM image is not fully under its nominal "owner's" control. The fact that a SafeNet HSM server does not notice when a VM moves allows smooth operation of the client that is using the resources of that HSM. The HSM server neither knows, nor cares, that its assigned client VM is moving (or not); the crucial concern is that that HSM server knows it is always talking to the right VM. The possibility of an unauthorized VM clone arises out of the portability and reproducibility of VMs in general. This is the virtual-world equivalent of an unauthorized person walking out of a server room with an application server.

The Unique Challenge

The challenge for an HSM serving virtual clients is to know that the HSM server is talking to the authorized instance of a virtual client, and no other. Virtual Machines in many cloud environments are 100% isolated from their physical

environment, therefore no physical attribute (not a TPM, nor a CPU ID, nor a MAC address) can be used to lock down the VM. Similarly, cloud-service metadata, like any data, is easily copied and manipulated, and therefore is not suitable as a link-securing characteristic.



What Is SafeNet Doing?

To protect against potential attacks, such as illustrated above, and to continue to offer “defense in depth”, SafeNet developed HTL, the Host Trust Link. HTL with its One-Time-Token solution is SafeNet’s built-in, HSM-based protection of HSM/Client registrations for cloud solutions.

With the VM decoupled from any specific piece of hardware or physical location, HTL uses a proprietary binding protocol to maintain the connection's association with a given VM regardless where that physical VM instantiation resides. The NTL service is still used, as before, but the new verification layer is added.

HTL supports two objectives:

- Ensure that a stored VM image, containing NTL credentials, cannot be cloned to establish an unauthorized NTLS connection to the SafeNet HSM server.
- Provide protection against cloning attacks after the VM binding has been established in a running VM.

The secret data used to protect the HTL link and ensure it cannot be spoofed or re-used is maintained only in RAM, which greatly increases the difficulty of an attack.

The Problem

When deploying clients in VM/Cloud environments, it is possible to pre-configure each VM with NTLS credentials (assuming that a unique IP address can be supplied for each set) and to provision both the client and an HSM partition when convenient. A virtual client can then be launched and begin interacting with a SafeNet HSM server over an NTLS link, without specific setup steps required for that VM. A clone of that pre-configured client VM, in the wrong hands, could work as well.

Our Solution

The HSM with HTL enabled will not allow an NTLS connection with a client instance until the Host Trust Link establishes that the client requesting NTLS is the correct VM instance of that client.

Once the VM is started and the HTL link is active, it might be possible for an internal attacker to make a complete copy of a running VM, in an attempt to impersonate the original client. The following layered protections mitigate potential concerns with respect to the provider security:

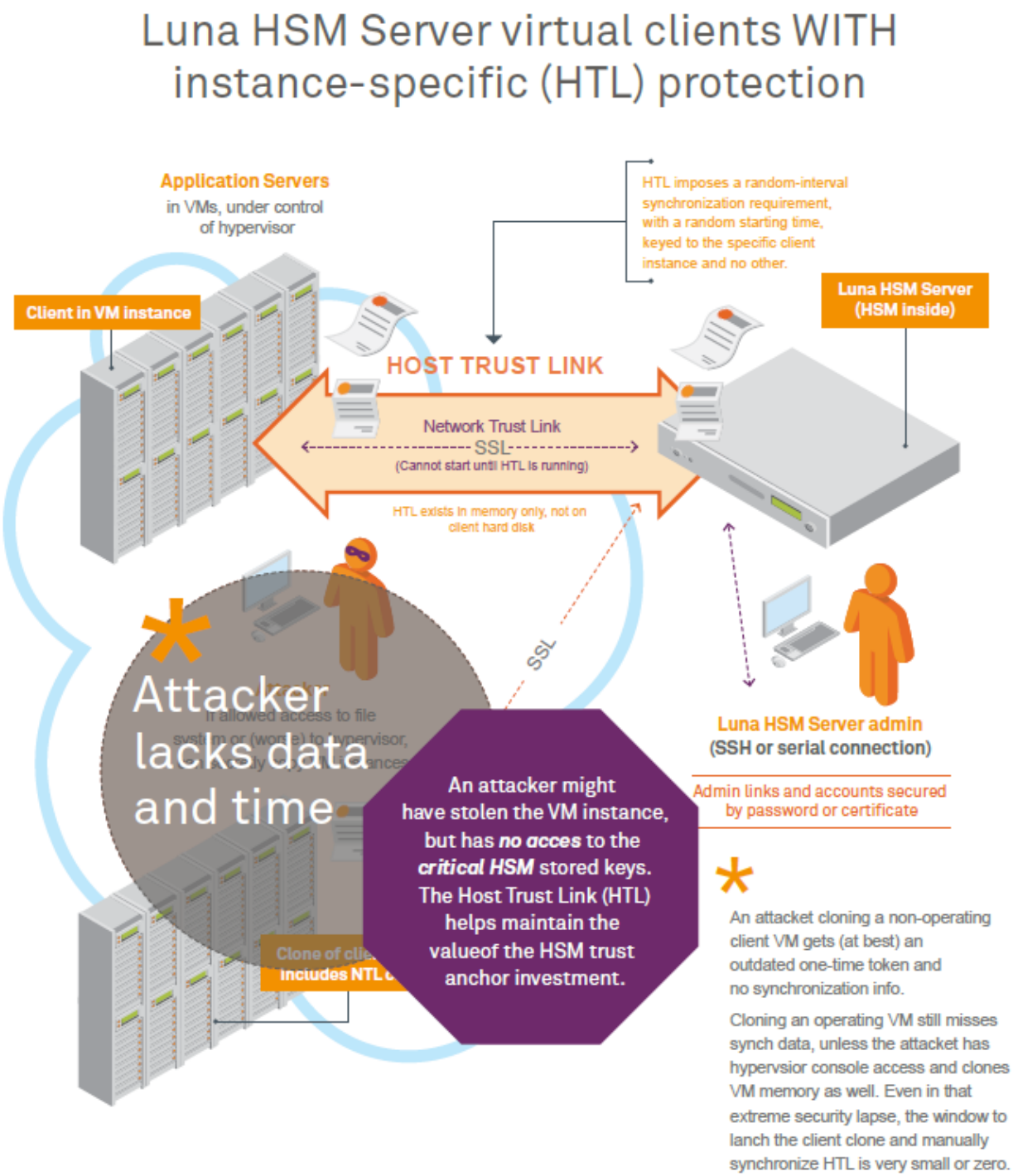
- **Binding to IP:** NTL binds the original VM to one IP address. If a clone of this VM is made with a different IP address, it will be unable to use the HSM. If a clone is made and assigned the same IP address, either the original VM would have to be killed (a noticeable event) or there would be network collisions (also detectable).
- **TLS encrypted communications:** All HTL counter values and synchronization packets are sent over a TLS link encrypted with a dynamically generated secret. This secret is in turn derived from a private key and certificate that are generated specifically for that VM instance during the HTL setup sequence. This arrangement makes it extremely unlikely that an attacker could use a cloned VM to “take over” an existing HTL connection as they would confront the hijacking protections of the TLS protocol.
- The binding protocol requires a **One Time Token (OTT)** from the SafeNet HSM appliance, generated specifically for that client instance. This prevents an attacker, cloning a VM at rest, from using the cloned image to connect to the SafeNet HSM.
- **Random data used in generating One Time Tokens** is derived from the HSM’s hardware Random Number Generator (RNG complying with NIST SP 800-90), assuring maximum randomness, and therefore highest quality input to the process.
- **One Time Token auto-refresh:** The HTL maintains a constantly changing synchronization code with the HSM

server, based on a random initial counter value and step interval assigned by the HSM, which allows the authorized instance to re-establish its HTL after brief periods. The length of this period is configurable by the HSM administrator and it defaults to 2 minutes. Administrators can lengthen the time for improved reliability if the network links are unreliable, or shorten the time to increase the overall security of the HTL.

When the HTL mode is active, then ANY way an attacker manages to obtain an unauthorized copy of the VM it will be rejected by the HSM (until it receives a valid One Time Token). For such an attack to succeed, the counter would need to be re-synchronized to match the original VM by manipulating its value in RAM. This attack might be possible, but the use of a random initial counter value, a random step interval, and the ongoing synchronization, presents a significant barrier.

If a client requires VM binding, and an existing HTL link for that client goes down, the HSM server kills all existing NTLS connections from that client. This action occurs immediately, and is independent of the grace period (if any).

A client user, using a supplied GUI tool, can check the status of the HTL link for every configured, registered appliance.



New opportunities, new threats – evolved protection

Why did we choose to create our own trust anchors to achieve the desired security when moving to a virtual environment, rather than relying on attributes available in the VM?

VMs are intended to be completely isolated from their physical environments. VM attributes are already difficult to find that

- are not static
- can reliably distinguish between VM instances, and
- are not easy to spoof.

The trend is toward greater isolation. HTL is a SafeNet-generated and controlled link-authentication protocol, independent of VM attributes. SafeNet OTT technology provides enhanced security for future clouds without giving up the benefits of the cloud.

In Which Environments Does SafeNet's HTL Protect?

HTL is introduced for the virtual environment because there is a pressing need to control a VM's ability to connect. However, HTL can also help in the non-virtual world. Some customers are concerned that an attacker could grab the NTL private key file from a legitimate physical server, move it to a rogue server, and connect from there -- a physical world version of the malicious VM clone. HTL can address that concern.

4

SafeNet HSM Product Security Features

SafeNet HSM products include a number of features that enhance security and allow you to configure aspects of security to fit your situation.

Some are decided at purchase time (example: does your HSM require Password authentication, or PED authentication). Others are determined during setup and configuration (example: "SO can reset Partition PIN" and "Force user PIN change after set/reset", both of which are HSM policy settings).

Further, certain policy changes in the HSM or in a Partition are destructive - meaning that any current contents are lost when the policy changes. This is considered a necessary security measure because those changes represent a modification of the security level of the HSM.

Another aspect of security is the manner in which different roles are separated - a given user or administrator can perform only a limited set of operations that fit within a defined role. Other roles have other responsibilities that do not overlap. The compartmentalization limits the scope of action of any one person, thus limiting possible damage if the holder of a single role is compromised. Of course, you can give all the passwords or all the PED Keys to just one person, if you like, but that would be a matter for your organization's security policy. If your security policy is silent on the matter, then it should be updated to address your use of HSMs.

The SafeNet HSM security features are described in the following sections:

Roles and Users

SafeNet HSM roles and authentications cover basic PKCS #11 roles, as well as some additional authentications to support SafeNet features.

Those roles and authentications have equivalents for Password-authenticated and for PED-authenticated SafeNet HSMs (with exceptions - see table).

Role or Feature	Format for Password Authenticated	Security and Control [see Note 1]	Format for PED Authenticated	Security and Control [see Note 2]	What if I lose/forget this?
HSM SO (HSM/admin level)	human-readable password string	Control access to the HSM. Must trust personnel or somehow control to whom they communicate the	Blue PED Key for administrative login at HSM level	Procedures needed to control and track who has access to the PED Key and to the HSM	HSM Administrator/ Security Officer (SO) cannot log in to perform any HSM-level

Role or Feature	Format for Password Authenticated	Security and Control [see Note 1]	Format for PED Authenticated	Security and Control [see Note 2]	What if I lose/forget this?
		password. Change the password whenever personnel depart, or the chain of control and trust lapses.			administration, including setting policies, creation or deletion of application partitions. Must re-initialize the HSM, losing all content.
Application Partition SO (PSO, single application partition level)	human-readable password string	Must trust personnel or somehow control to whom they communicate the password. Change the password whenever personnel depart, or the chain of control and trust lapses.	Blue PED Key for administrative login by partition SO at partition level	Procedures needed to control and track who has access to the PED Key and to the HSM	Application partition Security Officer (SO) cannot log in to perform any partition-level administration, including creation or deletion of Crypto Officer, adjusting policies, etc. Must re-initialize the partition, losing all content.
Cloning Domain (HSM/admin level, or per application partition)	human-readable domain string for setting or authenticating cloning domain between two or more HSMs, or two or more application partitions	Must trust personnel or somehow control to whom they communicate the cloning-domain string	Red PED Key for setting or authenticating cloning domain between two or more HSMs or two-or-more application partitions	Procedures needed to control and track who has access to the PED Key and to the HSM	Objects on any HSM or on any partition that shares this cloning domain can no longer be cloned to any other HSM or partition or token, including backup/restore or use in an HA group. HSM or partition must be re-initialized (losing all content) and a new cloning domain

Role or Feature	Format for Password Authenticated	Security and Control [see Note 1]	Format for PED Authenticated	Security and Control [see Note 2]	What if I lose/forget this?
					imprinted.
Crypto Officer (per application partition)	human-readable password string	Must trust personnel or somehow control to whom they communicate the password - client/application and CO have same password	Black PED Key for admin and role/partition Activation, plus human-readable password string for client app	Procedures needed to control and track who has access to the PED Key and to the HSM - the text string password for client/application keeps CO management function separate from operational use.	Application partition Crypto Officer (CO) cannot log in to perform any CO-level administration, including creation or deletion of CU role, or activation of partition for object-modifying operational access by application. PSO must re-create the CO role, losing any objects or subsidiary role that were created by the original CO role.
Crypto User (per application partition)	human-readable password string	Must trust personnel or somehow control to whom they communicate the password - client/application and CU have same password	Gray PED Key for admin and role/partition Activation, plus human-readable password string for client app	Procedures needed to control and track who has access to the PED Key and to the HSM - the text string password for client/application keeps CU management function separate from operational use.	Application partition Crypto Officer (CU) cannot log in to perform any CU-level administration, including activation of partition for object-using operational access by application. CO must re-create the CU role, losing any

Role or Feature	Format for Password Authenticated	Security and Control [see Note 1]	Format for PED Authenticated	Security and Control [see Note 2]	What if I lose/forget this?
					objects that were owned by that role.
Auditor (HSM level)	human-readable password string	Must trust personnel or somehow control to whom they communicate the password	White PED Key for administrative login to Audit function	Procedures needed to control and track who has access to the PED Key and to the HSM	Can no longer validate any logs created by that auditor. Existing logs still available (except for any records that were in the HSM, waiting to be exported to a log file), but you can no longer demonstrate trust for audit purposes. Create a new auditor.
Remote PED Key (RPK, HSM level)	N/A	N/A	N/A	Procedures needed to control and track who has access to the PED Key and to the HSM	Cannot perform PED operations remotely with any HSM that shared that RPK. Must generate a new RPK and imprint it on all HSMs that are to be accessed with it, and copies of the new orange PED Key must be brought to all Remote PEDs that will be used with those HSMs.
Secure Recovery Key (SRK, HSM level)	N/A	N/A	N/A	Procedures needed to control and track who has access to the PED Key and to the HSM	Cannot recover from hardware tamper events, or from Secure Transport Mode.

Role or Feature	Format for Password Authenticated	Security and Control [see Note 1]	Format for PED Authenticated	Security and Control [see Note 2]	What if I lose/forget this?
					If lost SRK was valid (meaning, that portion of the secret existed only on the lost PED Key, and not inside the HSM), then a new SRK cannot be created without return of HSM to Gemalto for re-manufacture; all contents are lost.

[Note 1: Always store a written copy of the string in a safe and secure lockup, in case security personnel who have memorized it become unavailable. Have a procedure for accessing that stored copy in time of need (including for updates when passwords are changed - does not apply to domain string, which cannot be changed). Gemalto has no way to recover your lost or forgotten authentication strings. See Note 3, below.]

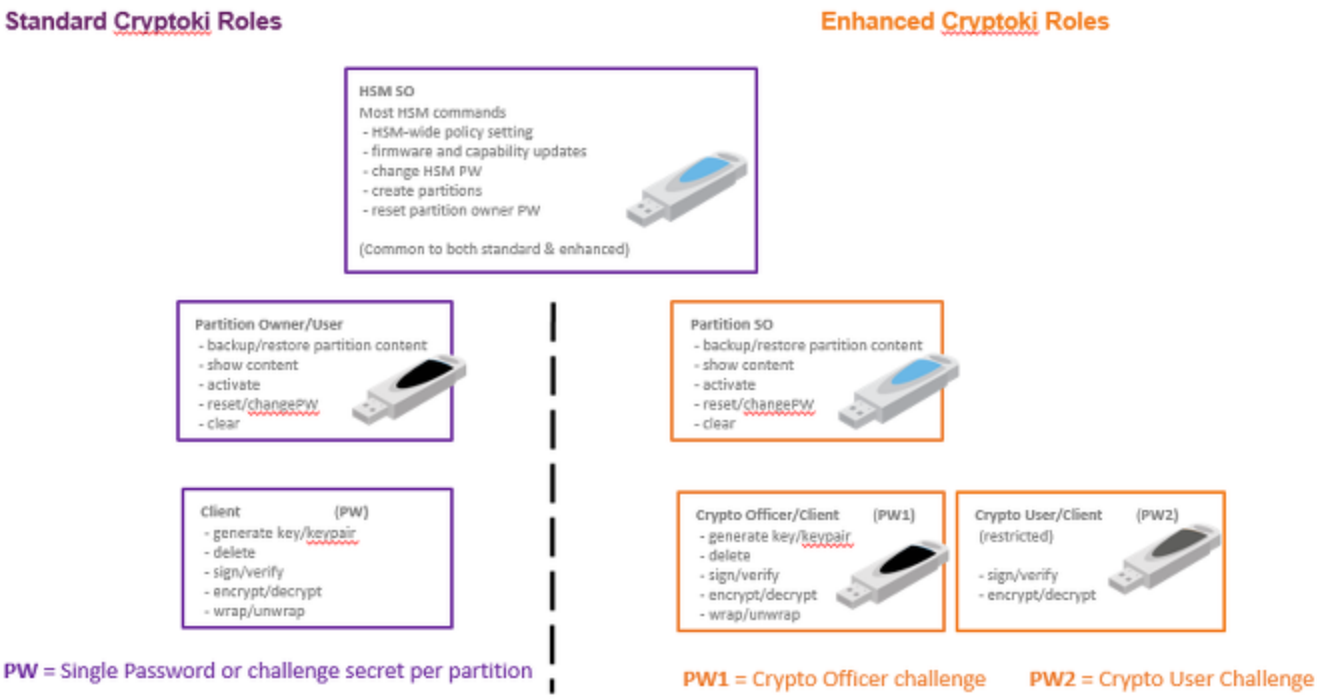
[Note 2: Always make sufficient copies of any important, imprinted PED Keys, sufficient to have at least one on-site backup copy (in secure storage) of each key, and at least one off-site backup copy (in secure storage) of each key. Gemalto has no way to recover lost PED Key data. See Note 3, below.]

[Note 3: The HSM does not store authentication secrets; it encrypts material using the authentication secrets. That material can be decrypted temporarily, for use, when those secrets are requested by the HSM and provided by you. The temporary decryption occurs in volatile memory, inside the HSM, and disappears with power loss or at end of session.]

Separation

A basic concept for cryptographic operations with HSMs is the separation of roles. For security and oversight, it is desirable to separate administrative functions from operational cryptographic functions. To that end, SafeNet HSM products support a variety of roles and users. The different types of HSM, and the options available to them, support a variety of operational and security regimes.

The following diagram summarizes the Cryptoki roles.



Note: In addition to providing the Crypto User password, a Client application must also pass the user type CKU_RESTRICTED_USER (or the alias CKU_CRYPTO_USER).

To work with a Partition as Crypto Officer, **OR** for applications that use the existing standard, your application must pass the user type CKU_USER (along with the Crypto Officer / Partition Owner password). However, this type now has an alias CKU_CRYPTO_OFFICER, which you might prefer to use for reasons of clarity. (This concerns you only if you are an application developer.)

Note: The **Partition SO** role exists only for HSMs with firmware 6.22.0 or newer, and with Per-Partition SO enabled.
For all other HSMs, the application partitions are administered by the HSM SO.

HSM General Authentication Model

This section discusses how objects are protected on the HSM, how authentication works, and how authentication credentials are protected.

The general authentication model applies to both Password Authenticated and PED Authenticated SafeNet HSMs. SafeNet 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 while needed.

One general storage key (GSK), for the HSM, protects general storage objects that might be needed by various roles in the performance of their duties. 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 the diagram below, is repeated for each role. The USK for

each separate role on the HSM encrypts objects that are owned by that role, ensuring that each person, authenticating as a role, sees and touches only what belongs to them.

Where is the password stored in the HSM, and how is it protected?

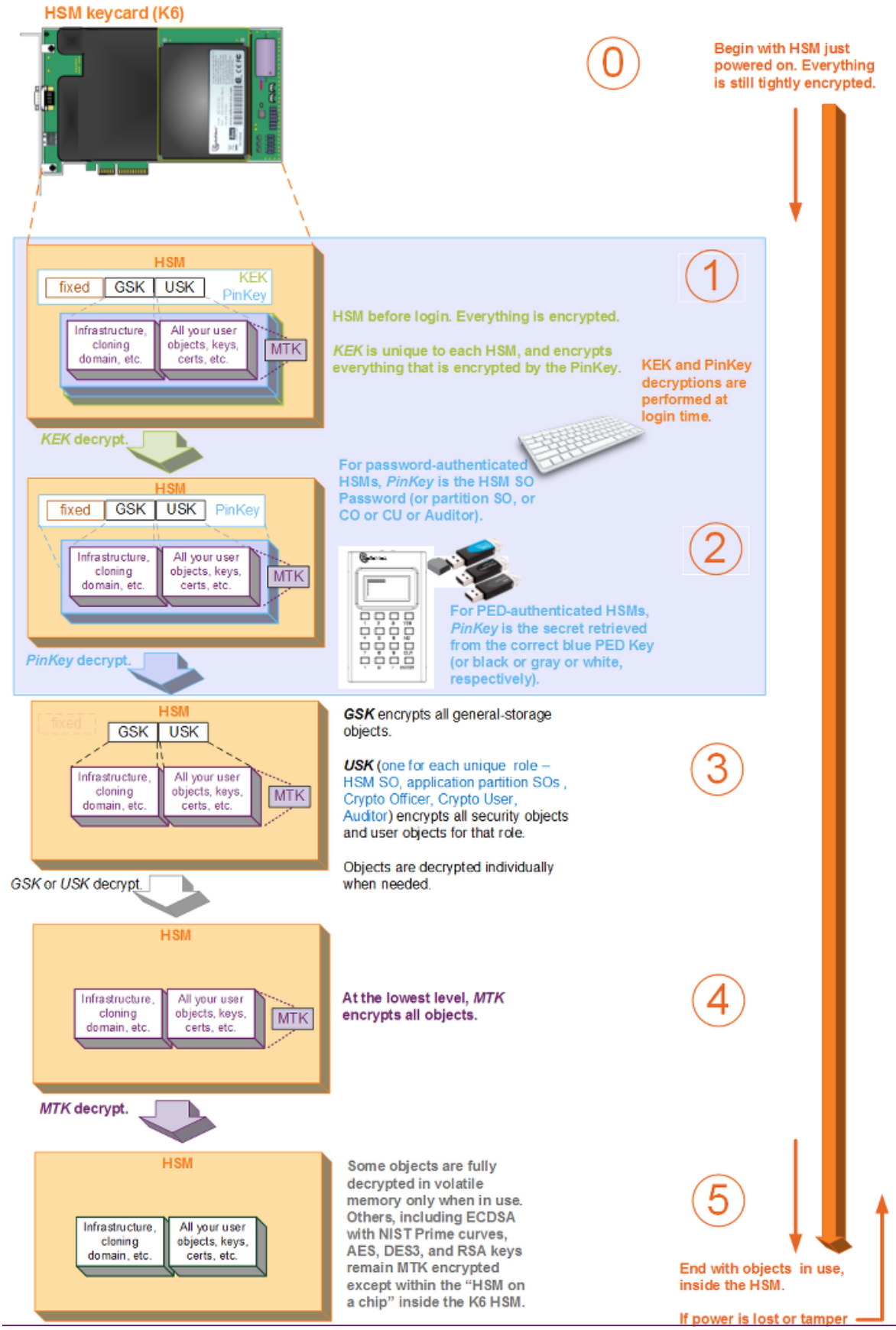
The password is ***not stored***; whether it is a true password for a Password-authenticated HSM, or is a PED Key value for a PED-authenticated HSM, the HSM does not keep a copy. For each partition, and the role that authenticates to it, the HSM has a checkword, an encrypted block consisting of a fixed value plus the GSK plus the appropriate USK. The encryption is derived from the PIN Key *for that role*. An operation using SHA-512 derives an AES key, then AES CBC is used to decrypt the checkword. If the fixed-value portion verifies, then the HSM proceeds to use the decrypted GSK and USK where needed in operations by that authenticated role, until the session ends.

If multiple roles for a given partition have access to the objects (for example, the Crypto Officer and Crypto User), then both their checkwords contain the same USK, but encrypted under their own respective credentials.

The Protection Model

For clarity, the following diagram depicts the general case, that applies to either Password-authenticated or PED-authenticated HSMs, without some of the optional features (MofN, PED PINs) that could additionally be invoked for some, or all, roles on a PED-authenticated HSM.

HSM Layered Encryption - the General Case



For a description, based on the above, but adding MofN split-knowledge, multi-person access control, see "HSM authentication model with MofN split secret" on page 1.

For a description, based on the above, but adding a PED PIN (something you know) to the secret contained on a physical PED Key (something you have), see "HSM Authentication with One PED PIN" on page 1.

For a description, based on the above, but showing the addition of both MofN and PED PINs, see "HSM Authentication Model with both PED PIN and MofN" on page 1.

About Capabilities and Polices

SafeNet HSMs are built on one of our general-purpose HSM platforms (hardware plus firmware), and then are loaded with what we call "personality", to make them into specific types of HSM with specific abilities and constraints, to suit different markets and applications. The built-in attributes are called "Capabilities" and describe what the HSM can do as it comes to you from the factory. Some capabilities are unalterable, except by re-manufacturing the HSM. Many HSM capabilities can be altered by means of HSM Policies, which coincide one-for-one with the capabilities that they alter.You can view the current HSM capabilities and policies with the **hsm showpolicies** command:You can change a current HSM policy in LunaSH with the **hsm changepolicy** command.You can change a current HSM policy in lunacm with the **hsm changeHMSPolicy** command.

Similarly, capabilities and policies for each HSM partition control the behavior and the security parameters of the partition.

If a capability governs a security parameter, then the respective policy can set the HSM or the HSM partition to be more restrictive than the base capability allows, but never less restrictive.

Policy change actions that materially affect the cryptographic security of the HSM or of a partition are "destructive", meaning that if you invoke a change to such a policy, all contents of the HSM (or of the partition) are destroyed. In such an event, you can create new versions of objects that were formerly on the HSM or in the partition, or you can restore from backup.

Refer to the Configuration Guide and the Administration Guide for further discussion and instruction around capabilities and policies.

About MofN

The MofN feature provides a means by which organizations employing cryptographic modules for sensitive operations can enforce multi-person control over access to the cryptographic module, or selected aspects of it. The feature is available in all SafeNet HSMs configured to use SafeNet PED, the PIN Entry Device (PED), and associated PED Keys for authentication.

MofN involves a splitting of an authentication secret into multiple parts or splits. The shared secret is distributed (or “split”) among several PED Keys (“split-knowledge access control”). Every type of PED-administered HSM authentication secret can be split when it is created:

- blue SO PED Key,
- red Cloning Domain PED Key,
- blue Partition SO PED Key,
- black Crypto Officer PED Key,
- gray Crypto User PED Key,
- orange Remote PED Vector Key,

- purple Secure Recover Key,
- white Audit PED Key.

How MofN works

For a non-PED-authenticated (that is, for Password authenticated) HSM, you could simulate a weak form of MofN by giving two persons (or more) each a portion of the text string to authenticate to a role or a function on the HSM. Then you would need a third person to oversee each authentication to ensure that the holders of the partial password strings entered them in the correct order and did not view each other's portions.

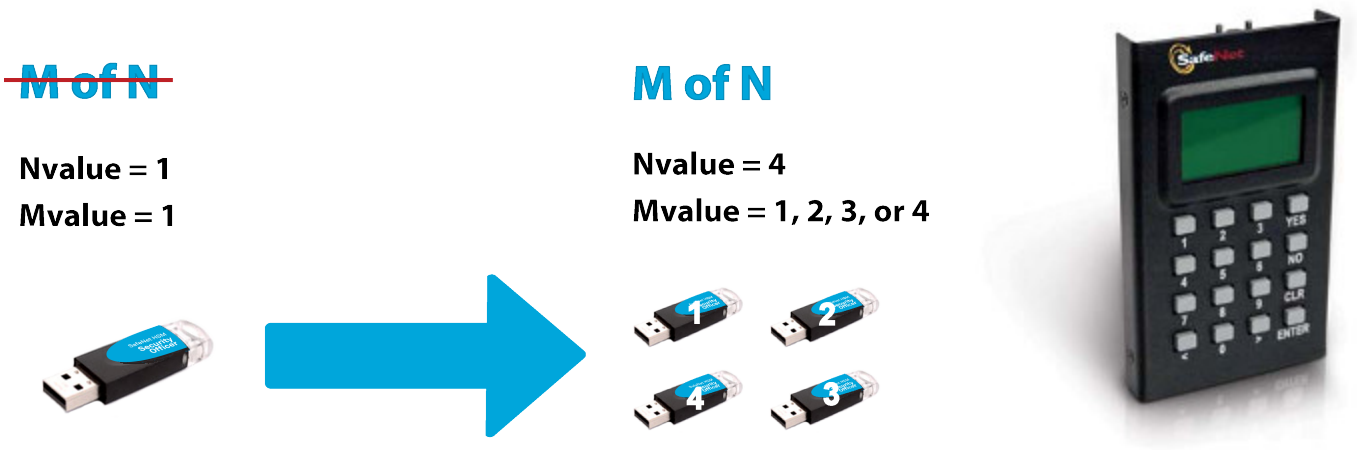
For PED-authenticated HSMs, real MofN is a much more robust, self-enforcing feature.

Without MofN, you can initialize an HSM such that you must produce just a single blue HSM Admin/SO PED Key in order to login and perform HSM management functions, and you must produce a single black Crypto Officer PED Key in order to activate a Partition to receive Client connections and allow Client applications to perform operations within the Partition, and similarly for any of the other roles and authentication secrets listed above. And that can be the extent of your security and oversight. If that is sufficient, you can stop reading this topic.

With MofN, the authentication secret contained on one blue SO PED Key or one black Crypto Officer PED Key (or red Domain key or gray Crypto User key or orange Remote PED key or purple Secure Recovery key or white Auditor key) is still necessary, but is no longer sufficient for authentication. Access now requires additional authentication by an overseer, or several overseers or cooperating co-key-holders. That additional oversight constitutes "M" holders of separate portions of the role secret, which is now the MofN "split knowledge shared secret". What that means is that the SO secret, or partition Crypto Officer secret, or cloning Domain (as well as the Remote PED secret and the Secure Recovery secret and the Audit secret and the Crypto User secret, if used) can be split into portions (over several PED Keys of the current color, rather than just one), and a defined number of those portions must be brought together in order to re-create the complete secret. One person, with one PED Key can no longer authenticate for an HSM role or function that has MofN set.

At initialization time, or role creation time, you are referred to the PED, where you get to specify into how many splits or shares each authentication secret is divided - this is quantity N (which can be any number from 1 to 16). You also specify how many of those splits or shares must be joined together by SafeNet PED in order to re-create the secret - this is the quantity M. M can be less than or equal to N. Specify those quantities by providing the "Nvalue" and the "Mvalue" when prompted by SafeNet PED. Those values become associated with the secret, and required, for the life of that secret - until you cause a new secret to be created. That might occur when changing or resetting a "password" (PED Key secret) for a role, or when generating a new Remote PED Vector, or generating a new Secure Recovery Vector. It could also occur if you factory reset, then re-initialized the HSM, but only if you chose not to reuse existing PED keysets (see "Reuse" below).

Creating an Authentication Secret Without MofN vs With MofN



In the above illustration, the right-hand side depicts the SO secret (could be HSM Admin/SO, or could be application partition SO in a per-partition SO context) split among four blue PED Keys. This is not four copies of a secret - this is four different pieces, or splits, of a single secret. As indicated, the Mvalue, the quantity of those splits that will be needed in any future authentication, could be set to any value between 1 and Nvalue (in this case 4).

- Setting M to 1 would be pointless. You might as well have set Nvalue to 1, also, and just made identical copies of that single complete-secret key for your spares.
- Setting Mvalue to 4 is valid, but requires that **all** holders of blue-key splits must be present whenever authentication is prompted - no blue-key holder can take vacation or sick-leave, or travel for business, without handing control of her/his split to an alternate responsible person, not one of the existing split-holders.
- Suitable Mvalue settings, when Nvalue is 4, would be either M=3 or M=2.

N=4 is just a handy example size. We could have used any nValue up to 16, but larger numbers would make for a more cumbersome example to explain the concept.

Authenticating

To log in or authenticate with MofN in force, you are first prompted to supply, for example, a blue PED Key (or a black PED Key, or whichever of the colors is appropriate to the task), then you are prompted to supply an additional (different) key of that color, from that set, and to repeat until M splits have been presented - those can be any M of those keys, in any order, as long as all are different. That is, the secret is spread over N keys, but you need only M of them to recreate the complete secret when required (where M is usually less than N).

As illustrated below, if you set MofN to N=4 and M=3, then any three of the set can be presented, when SafeNet PED prompts for SO login.

Secret splits 2, 3, and 4 (above) combine to reproduce the complete SO authentication secret.
Secret split 1 is grayed out, to indicate that you do not need it when authenticating, if you present 2, 3, and 4 when prompted by the PED.

Or, secret splits 1, 3, and 4 combine to reproduce the complete SO authentication secret, with 2 not needed.

Or, secret splits 1, 2, and 4 combine to reproduce the complete SO authentication secret, with 3 not needed.

Or, secret splits 1, 2, and 3 combine to reproduce the complete SO authentication secret, with 4 not needed.

From an MofN = 3of4 set, any of the above 3-PED-Key combinations will get you into that HSM or partition.

When seeking an MofN divided secret, SafeNet PED does not ask for a specific split. All it wants is a split that is a portion of the requested secret, but different from any previous splits you have offered, during this authentication attempt. When it successfully receives the number of different splits that are indicated in the PED Key header, the authentication attempt is made at the HSM.

Where and When to Use MofN

Use MofN when you want a selected type of HSM access to require the presence of more than one person. MofN is invoked per authentication secret. That is, it applies to only those secrets where you deliberately choose to invoke MofN as the secret is being created/imprinted. Thus you could have MofN multi-person control imposed for HSM SO and for Cloning Domain, but not for Partition Crypto Officer, nor SRK, nor RPV… or any other combination that made sense in your environment. Please review "How Many PED Keys Do I Need?" on page 1 before you make any decisions about invoking MofN for one-or-more authentication secrets for an HSM.

During initialization and administration of the HSM, the HSM Administrator or Security Officer [SO] invokes MofN if desired as the procedure reaches the point of creating/imprinting each authentication secret. The HSM SO supervises the imprinting of a blue PED Key or a set of N blue keys. The SO specifies how many shares (also sometimes called "splits") will make up the shared secret. This total number is N and may be any number up to 16. The SO then specifies how many of that total number of (current color) PED Keys are to be required at each login/authentication of the role or secret. This second number, M, can be any number up to N. During initialization, the SO would also be presented with the same choices for the HSM administrative partition's cloning domain.

From that point on, any future login or invocation of that particular authentication (blue key, or red key) to the HSM requires that quantity M of that-color share keys be provided. The result is that no single person can operate that aspect of the HSM.

The same choices then occur as an application partition is created and has roles and secrets created for it. One holder of the Crypto Officer key or the HSM Admin/SO key (for example) must bring together M different share-holders (including himself/herself), each with one of the black or blue keys, as appropriate, before the HSM or partition can be unlocked.

Again, the same applies to any of the other colors (roles/secrets), RPK, SRK, Auditor,for which MofN was invoked.

HSM Role or Secret	**Number of splits required per role/secret if one role/secret has MofN invoked**	
	Number of Splits created (N) [Note 1]	**Number of splits needed to authenticate (M)** [Note 2]
Blue - HSM Administrator or Security Officer (SO)	Any value from 1 to 16	Any value from 1 to N
Blue - Application Partition Security Officer (SO)	Any value from 1 to 16	Any value from 1 to N
Red - Cloning Domain	Any value from 1 to 16	Any value from 1 to N
Black - Crypto Officer (sometimes called application partition Owner for "legacy" partitions without Partition SO)	Any value from 1 to 16	Any value from 1 to N
Gray - Crypto User	Any value from 1 to 16	Any value from 1 to N
Orange - Remote PED Vector	Any value from 1 to 16	Any value from 1 to N
White - Auditor	Any value from 1 to 16	Any value from 1 to N
Purple - Secure Recovery Vector	Any value from 1 to 16	Any value from 1 to N
[Note 1 - Selecting an Nvalue of 1, when imprinting a role or secret, means no MofN splitting for that role/secret; a single PED Key unlocks that role or function. Selecting an Nvalue greater than 1, when imprinting a role or secret, means that secret is split across quantity N of that-color PED Keys.]		

HSM Role or Secret	Number of splits required per role/secret if one role/secret has MofN invoked	
	Number of Splits created (N) [Note 1]	**Number of splits needed to authenticate (M)** [Note 2]

[Note 2 - Mvalue is usually not selected as 1 (when N > 1), since that would mostly defeat the purpose of setting MofN.
Mvalue is usually not selected as N, since that leaves no scope to authenticate while one or more holders of secret-split PED Key is unavailable due to illness, vacation, business travel, or other reasons. Therefore, 1 < M < N is usually the case.]

The purpose of the above table is to emphasize explicitly that MofN settings are completely independent, per role or secret, on an HSM.

- Setting MofN, or not, for one role or function secret, has no influence on whether or not MofN can be set for any other role or secret.
- Setting Mvalue and Nvalue for one role or function secret has no influence on the values you might set for another.

What MofN is not

MofN is not a splitting of the private signing key; it is splitting of the SafeNet HSM's individual authentication/access secrets. That is, MofN is a splitting of the secret that lets you unlock a function of the HSM, but **not** a split of the working (encrypting, decrypting, signing, verifying) secrets - your keys and certificates - contained inside the HSM.

Note: In general, use MofN if you will be giving each split-containing PED Key to a different person. We recommend that you use MofN only if you have established a definite need for it. The additional security of split-knowledge, shared-secret, multi-person access control imposes additional administrative overhead, and increased possibility of making an administrative or handling error that could leave you unable to access your keys and certificates.

Reuse

When a PED Key contains an authentication secret from an HSM or partition, and you are imprinting a secret for a new HSM or partition, you are prompted to "Reuse an existing keyset?", or to overwrite any content of the PED Key (explained in detail at "Shared or Group PED Keys" on page 1).

If you present a PED Key containing a single split from an MofN set, the PED detects that it is viewing a partial secret, and prompts you for additional splits of that secret, in order to reproduce it and impose the reconstructed secret onto the current HSM (for that role). That is, you cannot use a single split from an MofN group as a complete secret on another HSM or partition. If the other HSM had MofN for that secret or role, and you choose to reuse, you must reuse all of it, and therefore you are choosing MofN for that role on the new HSM, just as it was on the original HSM.

Historical Note

In previous versions of SafeNet HSM, MofN was a selection made at the command-line (either lunash:> or lunacm:>) via the hsm init command. You could elect to use MofN or not, by means of options to the hsm init command. MofN, was a separate secret, spread across N green keys. If you invoked MofN, then it was always in force for that HSM (until the HSM was re-initialized). If you invoked MofN, it was in force HSM-wide. As explained above, modern MofN

behaves very differently, and we recommend taking time to understand the differences and implications if you are migrating from older SafeNet HSMs.

Tamper, Secure Transport, and Purple PED Keys

The HSM recognizes a number of tamper conditions (including over/under-temperature, physical interference, etc.), and allows you to choose how those are treated. The options range from simple reporting of an event in the HSM log, to temporarily (or even "permanently") disabling the HSM. In addition, the tamper function has been expanded to include Secure Transport Mode (STM) for ultimate security when shipping or storing your SafeNet HSMs. The advanced tamper features and ability to set STM are reserved for PED-authenticated SafeNet HSMs.

The use of purple PED Keys for tamper recovery is optional unless your security policy dictates that tamper events must require a response from the HSM's administrator, the Security Officer (SO).

The use of Secure Transport Mode (STM), which also uses the purple PED Key, is optional unless your security policy dictates that level of preparation before shipping or storage of the HSM.

If you wish to invoke Secure Transport Mode before shipping (or storing) a SafeNet HSM, you must enable the Secure Recovery Key (SRK). The SRK moves one of the two recovery splits (secure recovery vector or SRV) out of the HSM and imprints it onto a purple PED Key. The recovery splits are used to recover the Master Tamper Key in case it is destroyed by a tamper event or by invocation of STM. When you move one of those splits outside the HSM, you prevent automatic, hands-off recovery from a tamper event, and instead require that a purple-PED-Key holder must intervene to allow a tampered HSM (or one that was placed in Secure Transport Mode) to recover.

Those actions are described in detail elsewhere.

About the Purple SRK (secure recovery key)

Due to its nature, the purple PED Key (and its contained secret) behaves differently, in some respects, than all the other PED Keys.

- You choose to use this feature to enhance security during shipments or to enforce certain responses in case of physical tampering of the SafeNet HSM (once again, it is optional - you can use all other features of the HSM without ever invoking a purple PED Key). You must put safeguards in place to ensure that the SRK does not go missing - without the purple PED Key, you cannot recover from STM or a tamper event, and must ship the HSM back to SafeNet for re-manufacture.
- One of the safeguards that you can use is to make copies of the SRK at the time it is generated (*). If one of the copies is lost or destroyed, you can still recover the HSM.
- Another safeguard might be to extract the SRV onto multiple SRK splits (MofN greater than 1) rather than just one. If one of the N splits is lost or destroyed, you can still recover the HSM if you can locate quantity M of the remaining splits.
- As a safeguard against loss of the purple key in shipment, you do not need to ship the SRK to the site where the HSM is being installed. You can use Remote PED to perform the recovery from Secure Transport Mode. assuming that you have prepared the HSM and an orange Remote PED Key before the HSM is placed in Secure Transport Mode.

Unlike all other PED Keys, the purple PED Key cannot be duplicated via SafeNet PED's stand-alone duplication facility in the PED's Admin menu. If you attempt to do so, the PED insists that the source key you have presented is blank, and does not continue. Therefore, if you expect to need more than one copy of the SRK, you must make those

duplicates when the SRK is created - either at **hsm srk enable** or at **hsm srk keys resplit** for SafeNet Network HSM, or when using the lunacm commands **srk enable** or **srk generate** for SafeNet PCIe HSM and SafeNet USB HSM.

5
General Security Guidance

This chapter provides information about handling/storing/using your SafeNet HSM in secure fashion, and about ensuring that your network connections to the HSM and HSM host are as secure as possible. It contains the following sections:

About Connection Security

The following is not critical if your SafeNet systems reside inside secure locations, behind strong firewalls, and are managed only within/between such secured locations (via VPN for example).

However, if your application places the SafeNet appliance or HSM host in the "DMZ", please consider the following:

- Attackers are known to be making concerted efforts to compromise server administrator account passwords. Given research published over the past few years showing the capabilities of popular game console hardware, for example, to act as extremely fast brute force password generators, it is very likely that these recent attacks are making use of automated systems. For this reason, it is strongly recommended that particular attention be given to creating strong passwords for the HSM host system's accounts. If possible, pass-phrases of 15 characters or more should be considered. One established technique for generating pass-phrases is to select a phrase at random from a book, remove spaces and punctuation, and insert numeric and special characters to replace some of the letters. If you use this sort of technique, it is good to avoid some of the more common replacements such as capitalizing the first or last character in a word, replacing “e” with “3” or “s” with “$”, etc. since they would be the first ones tried by an attacker or password generator system.
- Given the sheer numbers of computer-using people in the world, any 'rule of thumb' that you can devise for streamlining your password-making has undoubtedly been thought of by someone else. If it's a rule, it can be automated, so assume that it has been automated by password-cracking programs everywhere. For example, look to the emerging "language" of text-message abbreviations for examples of substitutions that are already widely practiced and would therefore be easily cracked.
- Longer and more complicated passwords are progressively harder to crack, but they are also far more difficult to remember. Therefore long complicated passwords are more likely to need writing down, which drastically increases risk of exposure by means of 'social engineering' or simple detective work on the part of attackers.
- Currently the most secure text password seems to be a string of several **unrelated** words in your language of choice, preferably with no double characters, and totaling more than twenty characters. So, don't choose an unmodified phrase from a book. Your password should be nonsense, but nonsense that you can remember.
- For example *battery_trick$rapid6pink* - to get around the rule of "no doubles", you could insert a dash, or space or other character *bat-tery_trick$rapid6pink* but don't use that exact example - once this Help becomes public, that combination will be in a dictionary.

- Change the SSH port number from the well-known number 22 to something in the range of 1025 to 65535. Use the `lunash:>`**sysconf ssh port** command to change the SSH port number.

Consider Using Certificate-based Authentication

You can choose to use certificate-based authentication for your "admin", "operator", and "monitor" users (or named users with those roles) to connect, instead of password authentication. See the commands "sysconf ssh publickey" on page 1 and "my public-key" on page 1 in the *LunaSH Command Reference Guide* for details.

When creating your certificate on a client/admin computer, select a key size of 1024 bits or greater to generate the certificate.

Note that because the certificate resides on a computer, it is ultimately only as secure as access to that computer, which is likely protected by password (see above).

DRAFT SP 800-118 Guide to Enterprise Password Management

NIST announced that Draft Special Publication (SP) 800-118, Guide to Enterprise Password Management, has been released for public comment. SP 800-118 is intended to help organizations understand and mitigate common threats against their character-based passwords. The guide focuses on topics such as defining password policy requirements and selecting centralized and local password management solutions.

http://csrc.nist.gov/publications/PubsDrafts.html#800-118

Security and Handling Considerations - HSM Appliance

This section discusses general security and handling issues related to the SafeNet Network HSM appliance.

Physical Security of the Appliance

The HSM appliance is a commercial-grade secure appliance. This means that:

- It is provided with anti-tamper external features that make physical intrusion into the unit difficult - tamper-resistant screws must be drilled out, in order to open the case, and tamper-evident stickers secure the seams. These measures do not deter a determined attacker, they merely deter casual intrusion and leave visible evidence of attempts (successful or otherwise) to open the unit.
- Vents and other paths into the unit are baffled to prevent probing from the outside.
- The HSM Keycard, inside the appliance, that houses the actual HSM components, is encased in an aluminum shell, filled with hardened epoxy. Attempts to gain access to the circuit board itself would result in physical evidence of the attempted access and likely physical destruction of the circuitry and components, thus ensuring that your keys and sensitive objects are safe from an attacker.

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 managed 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.

Physical Environment Issues

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 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.

Communication

Communications with the unit are either local and, therefore, subject to direct oversight and control (you decide who is allowed to connect to the serial port or the PED port) or via secure remote links. All remote communications are as secure as SSH and TLS with tunneling protocol can make them.

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.

HSM Audit Data Monitoring

The HSM Keycard of the SafeNet HSM appliance stores a record of past operations that is suitable for security audit review. The easiest way in which to retrieve this record is to use the "`hsm supportinfo`" command and extract the dual port data provided within the `supportinfo.txt` file that is returned by the command. Because of the limited storage capacity of the HSM card, it has a limited size window in which to write these records and it must periodically re-start from the beginning of the window and overwrite existing records. For this reason, it is important that the audit data be retrieved often enough to ensure no data loss. Under typical load conditions, retrieving the file once every eight hours should be sufficient. However, for very heavy loads or operations containing large input data payloads, it might be necessary to retrieve the file as often as once per hour.

Audit Logging

Beginning with SafeNet HSM 5.2, the secure Audit Logging feature provides an Audit role (white PED Key) separate from all other HSM roles, to manage a secure audit logging function. 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.

Intended Installation Environment

The following assumptions are made about the environment in which the SafeNet cryptographic modules will be located and installed:

- Those responsible for the SafeNet HSM must ensure that the authentication data for each SafeNet HSM account is held securely and not disclosed to persons not authorized to use that account.
- Those responsible for the SafeNet HSM must ensure that it is installed, managed, and operated in a manner that is consistent with the local security policy.
- The host IT environment must be configured and checked to ensure that any applications installed in the host environment, that require access to the HSM are legitimate, are valid and have been vetted for authenticity and integrity (i.e., have not been modified for malicious purposes).
- Those responsible for the SafeNet HSM must ensure that it is installed and operated in an environment that is protected from unauthorized physical access.
- Those responsible for the SafeNet HSM must ensure that there are procedures in place such that, after a system failure or other discontinuity, recovery of the SafeNet HSM and the host IT environment is possible without compromise of IT security.
- Those responsible for the SafeNet HSM must ensure that those using the SafeNet HSM (including Security Officers and Token/Partition Users), have a level of competence sufficient to ensure its correct management and operation. This competence may be established through a combination of training and the accompanying Installation Guide and Configuration, Administration, and Reference documentation.
- Procedural and physical measures must prevent the disclosure of cryptography-related IT assets to unauthorized individuals or users via the electromagnetic emanations of the SafeNet HSM .
- Those responsible for the host IT environment must ensure that no connections are provided to outside systems or users that would undermine IT security.
- Those responsible for the host IT environment must ensure that the power supplied to the SafeNet HSM is adequately protected against unexpected interruptions and the effects of surges and voltage fluctuations outside the normal operating range of the device.
- Those responsible for the host IT environment must ensure that the SafeNet HSM is operated in an environment in which there is provided adequate protection against disasters such as fire and flood.
- Those responsible for the host IT environment must ensure that the SafeNet HSM is located in an environment that is adequate to protect security-relevant and cryptographic key data and the SafeNet HSM firmware from interference or inadvertent modification by strong electromagnetic radiation from other sources.

Security and Handling Issues - SafeNet HSM

This section chapter discusses general security and handling issues related to the SafeNet HSM and its host computer.

Physical Security of the Cryptographic Module

The SafeNet cryptographic module is a multi-chip standalone module as defined by FIPS PUB 140–2 section 4.5. 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 a SafeNet HSM, and apply the resources of a well-equipped engineering lab, it might be possible to breach its physical security. However, without the Password (password authenticated module) or the PED Keys (PED-authenticated module), such an attacker would be unable to decipher any signal or data that they managed to extract.

It is your responsibility to ensure the physical security of the module 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 cryptographic module and its authentication secrets.

It is your responsibility to ensure the physical security (access) of passwords or PED Keys, 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.

Physical Environment Issues

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 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.

Intended Installation Environment

The following assumptions are made about the environment in which the SafeNet cryptographic modules will be located and installed:

- Those responsible for the SafeNet HSM must ensure that the authentication data for each SafeNet HSM account is held securely and not disclosed to persons not authorized to use that account.
- Those responsible for the SafeNet HSM must ensure that it is installed, managed, and operated in a manner that is consistent with the local security policy.
- The host IT environment must be configured and checked to ensure that any applications installed in the host environment, that require access to the HSM are legitimate, are valid and have been vetted for authenticity and integrity (i.e., have not been modified for malicious purposes).
- Those responsible for the SafeNet HSM must ensure that it is installed and operated in an environment that is protected from unauthorized physical access.
- Those responsible for the SafeNet HSM must ensure that there are procedures in place such that, after a system failure or other discontinuity, recovery of the SafeNet HSM and the host IT environment is possible without compromise of IT security.
- Those responsible for the SafeNet HSM must ensure that those using the SafeNet HSM (including Security Officers and Token/Partition Users), have a level of competence sufficient to ensure its correct management and operation. This competence may be established through a combination of training and the accompanying Installation Guide and Configuration, Administration, and Reference documentation.

- Procedural and physical measures must prevent the disclosure of cryptography-related IT assets to unauthorized individuals or users via the electromagnetic emanations of the SafeNet HSM .
- Those responsible for the host IT environment must ensure that no connections are provided to outside systems or users that would undermine IT security.
- Those responsible for the host IT environment must ensure that the power supplied to the SafeNet HSM is adequately protected against unexpected interruptions and the effects of surges and voltage fluctuations outside the normal operating range of the device.
- Those responsible for the host IT environment must ensure that the SafeNet HSM is operated in an environment in which there is provided adequate protection against disasters such as fire and flood.
- Those responsible for the host IT environment must ensure that the SafeNet HSM is located in an environment that is adequate to protect security-relevant and cryptographic key data and the SafeNet HSM firmware from interference or inadvertent modification by strong electromagnetic radiation from other sources.

