THALES

SafeNet Luna PCIe HSM Client 10.1

CONFIGURATION GUIDE

Document Information

Product Version	10.1
Document Part Number	007-000555-001
Release Date	23 January 2020

Revision History

Revision	Date	Reason
Rev. A	23 January 2020	Initial release

damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

Regulatory Compliance

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

USA, FCC

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

Canada

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

Europe

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

CONTENTS

PREFACE: About the Configuration Guide

This document describes how to configure your HSM to get it ready to operate in your environment. Some of the following procedures are required before you can place the HSM in operation; others are optional. Some decisions are required at each stage.

The first task is to initialize the HSM, and assign a Security Officer to oversee and administer the HSM. Then you can apply some optional global settings. Next you will create application partitions, that your application will access to create, store, and use keys, certificates, and other crypto objects. A Partition Security Officer (SO) is assigned to each partition, and the HSM SO has no further access to the partition's contents. The Partition SO sets policies and performs other administration within the application partition, and assigns a Crypto Officer to handle access-control by applications.

Configuring an HSM consists of:

- Initializing the HSM - establishing ownership on the part of a role called the HSM Security Officer (SO). See "HSM Initialization" on page 9.
- Setting HSM Policies - configuration settings to adjust some security and behavior parameters. See "Set the HSM Policies" on page 20.
- Creating a working space on the HSM for your application programs, called an application partition. See "Creating an Application Partition on the HSM" on page 31.
- Set partition policies as desired. See "Setting SafeNet Luna PCIe HSM Partition Policies" on page 45.
- Perform any optional configuration tasks. See "Optional Configuration Tasks" on page 48.

The preface 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 from the Technical Support Customer Portal at https://supportportal.gemalto.com.

Audience

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

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

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

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

Notes

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

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

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

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

Support Contacts

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

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

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

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

Telephone

The support portal also lists telephone numbers for voice contact. (KB0013367)

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: HSM Initialization

Initialization prepares a new HSM for use, or an existing HSM for reuse, as follows. You must initialize the HSM before you can generate or store objects, allow clients to connect, or perform cryptographic operations:

- On a new HSM or factory-reset HSM, initialization sets the HSM SO credentials, the HSM label, and the cloning domain of the HSM Admin partition. This is often referred to as a 'hard' initialization. See "Initializing a New or Factory-reset HSM" on the next page.
- On an existing, non-factory-reset HSM, reinitialization destroys all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. This is often referred to as a 'soft' initialization. See "Re-initializing an Existing, Non-factory-reset HSM" on page 12.

> **NOTE** To ensure accurate auditing, perform initialization only after you have set the system time parameters (time, date, time zone, use of NTP (Network Time Protocol). You can use the **-authtimeconfig** option when initializing the HSM to require HSM SO authorization of any time-related changes once the HSM is initialized.

Hard versus soft initialization

The following table summarizes the differences between a hard and soft initialization.

Condition/Effect	Soft init	Hard init
HSM SO authentication required	Yes	No
Can set new HSM label	Yes	Yes
Creates new HSM SO identity	No	Yes
Creates new Domain	No	Yes
Destroys partitions	Yes	No (none exist to destroy, since the HSM is new or an **hsm factoryreset** was performed)
Destroys objects	Yes	No (none exist to destroy, since the HSM is new or an **hsm factoryreset** was performed)

Initializing a New or Factory-reset HSM

> **NOTE** New HSMs are shipped in Secure Transport Mode (STM). You must recover the HSM from STM before you can initialize the HSM. See "To initialize a new or factory-reset HSM (hard init)" on the next page for details.

On a new, or factory reset HSM (using **hsm factoryreset**), you perform a 'hard init' to set the following:

HSM Label	The label is a string that identifies this HSM unit uniquely. The HSM label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}|/;:'",.<>?`~` Spaces are allowed; enclose the label in double quotes if it includes spaces. Including both spaces and quotation marks in a label may cause unexpected labeling behavior. For more information, refer to "Name, Label, and Password Requirements" on page 1.
HSM SO credentials	For Multi-factor, or PED-authenticated HSMs, you create a new HSM SO (blue) PED key(set) or re-use an existing key(set) from an HSM you want to share credentials with. If you are using PED authentication, ensure that you have a PED key strategy before beginning. See "PED Authentication" on page 1. For password-authenticated HSMs, you specify the HSM SO password. For proper security, it should be different from the appliance admin password, and employ standard password-security characteristics. In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}|/;:',.<>?`~` Double quotation marks (") are problematic and should not be used in passwords. Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

Cloning domain for the HSM Admin partition	The cloning domain is a shared identifier that makes cloning possible among a group of HSM partitions. It specifies the security domain (group of HSM partitions) within which the HSM Admin partition can share cryptographic objects though cloning, backup/restore, or in high availability configurations. Note that the HSM Admin partition cloning domain is independent of the cloning domain specified when creating application partitions on the HSM. For Multi-factor, PED-authenticated HSMs, you create a new Domain (red) PED key(set) or re-use an existing key(set) from an HSM you want to be able to clone with. For password-authenticated HSMs, you create a new domain string or re-use an existing string from an HSM you want to be able to clone with. The domain string must be 1-128 characters in length. The following characters are allowed: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*-_=+[]{}/:',.~` The following characters are problematic or invalid and must not be used in a domain string: `"&;<>\`|()` Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks. **NOTE** Always specify a cloning domain when you initialize a Password-authenticated SafeNet Luna HSM in a production environment. The HSM allows you to specify "defaultdomain" at initialization, the factory-default domain. This is deprecated, as it is insecure. Anyone could clone objects to or from such an HSM. The default domain is provided for benefit of customers who have previously used the default domain, and for migration purposes. When you prepare a SafeNet Luna HSM to go into service in a real production environment, always specify a proper, secure domain string when you initialize the HSM.

To initialize a new or factory-reset HSM (hard init)

CAUTION! Ensure that you are prepared. Once initialized, re-initializing the HSM forces the deletion of all partitions and objects on the HSM.

1. If Secure Transport Mode is set, you must unlock the HSM before proceeding. New SafeNet Luna HSMs are shipped from the factory in Secure Transport Mode (STM). STM allows you to verify whether or not an HSM has been tampered while it is not in your possession, such as when it is shipped to another location, or placed into storage. See "Secure Transport Mode" on page 1 in the *Administration Guide* for more information.

   To recover your HSM from Secure Transport Mode, proceed as follows:

   a. As part of the delivery process for your new HSM, you should have received an email from Thales Client Services, containing two 16-digit strings, as follows. You will need both of these strings to recover the HSM from STM:

      Random User String: XXXX-XXXX-XXXX-XXXX

      Verification String: XXXX-XXXX-XXXX-XXXX

   b. Ensure that you have the Random User String and Verification String that were emailed to you for your new HSM.

c. Enter the following command to recover from STM, specifying the Random User String that was emailed to you for your new HSM:

   lunacm:> **stm recover -randomuserstring** <XXXX-XXXX-XXXX-XXXX>

d. You are presented with a verification string. If the verification string matches the original verification string emailed to you for your new HSM, the HSM has not been tampered, and can be safely deployed. If the verification string does not match the original verification string emailed to you for your new HSM, the HSM has been tampered while in STM. If the verification strings do not match, contact Thales Group Technical Support immediately.

e. Enter **proceed** to recover from STM (regardless of whether the strings match or not), or enter **quit** to remain in STM.

2. If you are initializing a Multi-factor-authentication (PED-authenticated) HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see "Changing Modes" on page 1 in the *HSM Administration Guide*. Alternatively, have a Remote PED instance set up, see "About Remote PED" on page 1.
3. Open a LunaCM session and set the slot to the HSM Admin partition.
4. Run the **hsm init** command, specifying a label for your SafeNet Luna PCIe HSM:

   lunacm:> **hsm init -label** <label>

5. Respond to the prompts to complete the initialization process:
   - on a password-authenticated HSM, you are prompted for the HSM password and for the HSM Admin partition cloning domain string (cloning domains for application partitions are set when the application partitions are initialized).
   - on a Multi-factor-authenticated (PED-authenticated) HSM, you are prompted to attend to the PED to create a new HSM SO (blue) PED key for this HSM, re-use an HSM SO PED key from an existing HSM so that you can also use it to log in to this HSM, or overwrite an existing key with a new PED secret for use with this HSM. You are also prompted to create, re-use, or overwrite the Domain (red) PED key. You can create MofN quorum keysets and duplicate keys as required. See "PED Authentication" on page 1 for more information.

   The prompts are self-explanatory. New users (especially those initializing a PED-authenticated HSM) may want to refer to the following examples for more information:

   - "PED-authenticated HSM Initialization Example" on the next page
   - "Password-authenticated HSM Initialization Example" on page 18

Re-initializing an Existing, Non-factory-reset HSM

On an existing, non-factory-reset HSM, re-initialization clears all existing partitions and objects, but retains the SO credentials and cloning domain. You have the option to change or retain the existing label. Re-initialization is also referred to as a soft init. If you do not want to do a soft init, and also change the SO credentials and cloning domain, you need to use the **hsm factoryreset** command to factory reset the HSM, and then perform the procedure described in "Initializing a New or Factory-reset HSM" on page 10.

CAUTION! Ensure you have backups for any partitions and objects you want to keep, before reinitializing the HSM.

To re-initialize an existing, non-factory-reset HSM (soft init)

1. Log in as the HSM SO.
2. If Secure Transport Mode is set, you must unlock the HSM before proceeding. See "Secure Transport Mode " on page 1 in the *Administration Guide*.
3. If you are initializing a PED-authenticated HSM, have the Luna PED connected and ready (via USB, in Local PED-USB mode). If your PED is not in USB mode, see "Changing Modes" on page 1 in the *HSM Administration Guide*.
4. Open a LunaCM session and set the slot to the HSM Admin partition.
5. Run the **hsm init** command, specifying a label for your SafeNet Luna Network HSM:

   lunacm:> **hsm init -label** <label>

PED-authenticated HSM Initialization Example

This section provides detailed examples that illustrate your options when initializing a PED-authenticated HSM. It provides the following information:

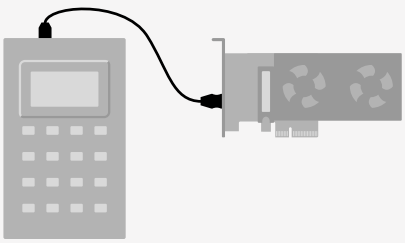
> "To initialize a PED-authenticated HSM" below
> "Imprinting the Blue HSM SO PED Key" on page 15
> "Imprinting the Red Cloning Domain PED Key" on page 16
> "New, reuse, and overwrite options" on page 17

NOTE Respond promptly to avoid PED timeout Error. If the PED has timed out, press the **CLR** key for five seconds to reset, or switch the PED off, and back on, to get to the “Awaiting command....” state before re-issuing a LunaSH command that invokes the PED.

To initialize a PED-authenticated HSM

1. Your Luna PED must be connected to the HSM, either locally/directly in USB mode (see "Changing Modes" on page 1), or remotely via Remote PED connection (see "About Remote PED" on page 1).

NOTE To operate in Local PED-USB mode, the PED must be connected directly to the HSM card's USB port, and not one of the other USB connection ports on the host system.

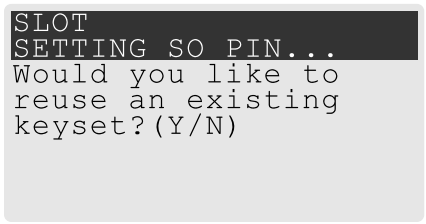


2. Set the active slot to the SafeNet Luna PCIe HSM Admin partition, and issue the **hsm init** command. The HSM passes control to the Luna PED, and the command line directs you to attend to the PED prompts.
3. When you issue the **hsm init** command, the HSM passes control to the Luna PED, and the command line (lunash:>) directs you to attend to the PED prompts.
4. A "default" login is performed, just to get started (you don't need to supply any authentication for this step).
5. Luna PED asks: "Do you wish to reuse an existing keyset?". If the answer is **No**, the HSM creates a new secret which will reside on both the HSM and the key (or keys) that is (or are) about to be imprinted. If the answer is **Yes**, then the HSM does not create a new secret and instead waits for one to be presented via the PED.
6. Luna PED requests a blue PED key. It could be blank to begin with, or it could have a valid secret from another HSM (a secret that you wish to preserve), or it could have a secret that is no longer useful.
7. Luna PED checks the key you provide. If the PED key is not blank, and your answer to "...reuse an existing keyset" was **Yes**, then Luna PED proceeds to copy the secret from the PED key to the HSM.
8. If the key is not blank, and your answer to "...reuse an existing keyset" was **No**, then the PED inquires if you wish to overwrite its contents with a new HSM secret. If the current content of the key is of no value, you say **Yes**. If the current content of the key is a valid secret from another HSM (or if you did not expect the key to hold any data) you can remove it from the PED and replace it with a blank key or a key containing non-useful data, before you answer **Yes** to the 'overwrite' question.
9. Assuming that you are using a new secret, and not reusing an existing one, Luna PED asks if you wish to split the new HSM secret. It does this by asking for values of "M" and "N". You set those values to "1" and "1" respectively, unless you require MofN split-secret, multi-person quorum access control for your HSM (See "M of N Split Secrets" on page 1 for details).
10. Luna PED asks if you wish to use a PED PIN (an additional secret; see "PED Key Management" on page 1 for more info).
11. If you just press **Enter** (effectively saying 'no' to the PED PIN option), then the secret generated by the HSM is imprinted on the PED key, that same secret is retained as-is on the HSM, and the same secret becomes the piece needed to unlock the Security Officer/HSM Admin account on the HSM.
12. If you press some digits on the PED keypad (saying 'yes' to the PED PIN option), then the PED combines the HSM-generated secret with your PED PIN and feeds the combined data blob to the HSM. The HSM throws away the original secret and takes on the new, combined secret as its SO/HSM Admin secret.
13. The PED key contains the original HSM-generated secret, but also contains the flag that tells the PED whether to demand a PED PIN (which is either no digits, or a set of digits that you supplied, and must supply at all future uses of that PED key).
14. Luna PED gives you the option to create some duplicates of this imprinted key. You should make at least one duplicate for backup purposes. Make additional duplicates if your security policy permits, and your procedures require them.
15. Next, Luna PED requests a red Domain PED key. The HSM provides a cloning Domain secret and the PED gives you the option to imprint the secret from the HSM, or to use a domain that might already be on the key. You choose appropriately. If you are imprinting a new Domain secret, you have the same opportunities to split the secret, and to apply a PED PIN "modifier" to the secret. Again, you are given the option to create duplicates of the key.
16. At this point, the HSM is initialized and Luna PED passes control back to LunaCM.

Further actions are needed to prepare for use by your Clients, but you can now log in as SO/HSM Admin and perform HSM administrative actions.

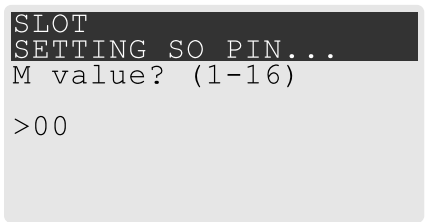
Imprinting the Blue HSM SO PED Key

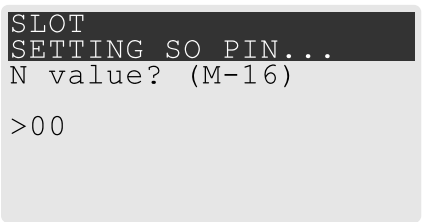
1. Decide if you want to reuse a keyset.



   - If you say **No** (on the PED keypad), then you are indicating there is nothing of value on your PED keys to preserve, or you are using blank keys.
   - If you say **Yes**, you indicate that you have a PED key (or set of PED keys) from another HSM and you wish your current/new HSM to share the authentication with that other HSM. Authentication will be read from the PED key that you present and imprinted onto the current HSM.

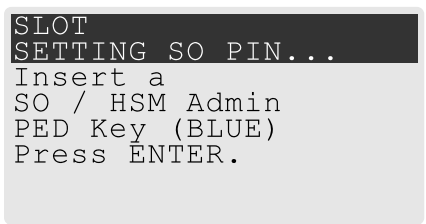
2. Set MofN.





   - Setting M and N to **1** means that the role authentication is not to be split, and only a single PED key will be necessary when the authentication is called for in future. Input **1** for each prompt if you do not want to use MofN.
   - Setting M and N to larger than 1 sets a quorum requirement for the role, which means that the authentication is split into N different splits, of which quantity M of them (the quorum) must be presented each time you are required to authenticate. MofN allows you to enforce multi-person access control - no single person can access the HSM without cooperation of a quorum of other holders.

3. Insert your blank key or the key you wish to overwrite.



   Insert a blue HSM Admin/SO PED key and press **Enter**.

```
SLOT
SETTING SO PIN...
   ** WARNING **
This PED Key is
blank.
Overwrite? YES/NO
```

- **Yes**: If the PED should overwrite the PED key with a new SO authentication.
  If you overwrite a PED key that contains authentication secret for another HSM, then this PED key will no longer be able to access the other HSM, only the new HSM that you are currently initializing with a new, unique authentication secret .
- **No**: If you have changed your mind or inserted the wrong PED key.

4. For any situation other than reusing a keyset, Luna PED now prompts for you to set a PED PIN. For multi-factor authentication security, the physical PED key is "something you have." You can choose to associate that with "something you know," in the form of a multi-digit PIN code that must always be supplied along with the PED key for all future HSM access attempts.

```
SLOT
SETTING SO PIN...
Enter new PED PIN:
*********
Confirm new PED PIN:
*********
```

Type a numeric password on the PED keypad, if you wish. Otherwise, just press **Enter** twice to indicate that no PED PIN is desired.

5. Decide if you want to duplicate your keyset.

```
SLOT
SETTING SO PIN...
Are you duplicating
this keyset?(Y/N)
```

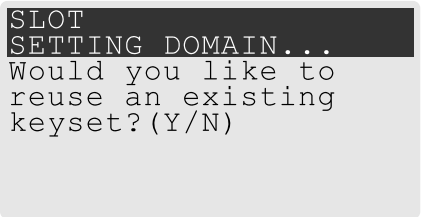
- **Yes**: Present one or more blank keys, all of which will be imprinted with exact copies of the current PED key's authentication.
- **No**: Do not make any copies.

> **NOTE** You should always have backups of your imprinted PED keys, to guard against loss or damage.

Imprinting the Red Cloning Domain PED Key

To begin imprinting a Cloning Domain (red PED key), you must first log into the HSM. Insert your blue SO PED key.

1. Decide if you want to reuse a keyset.



- **No**: If this is your first SafeNet Luna HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized
- **Yes**: If you have another HSM and wish that HSM and the current HSM to share their cloning Domain.

2. Set MofN.
   - Setting M and N to **1** means that the domain authentication is not to be split, and only a single PED key will be necessary when the authentication is called for in future. Input **1** for each prompt if you do not want to use MofN.
   - Setting M and N to larger than 1 sets a quorum requirement for the domain, which means that the authentication is split into N different splits, of which quantity M of them (the quorum) must be presented each time you are required to provide the domain. MofN allows you to enforce multi-person access control - no single person can access the HSM without cooperation of a quorum of other holders.
3. Insert your blank key or the key you wish to overwrite.
4. Optionally set a PED PIN.
5. Decide if you want to duplicate your keyset.

Once you stop duplicating the Domain key, or you indicate that you do not wish to make any duplicates, Luna PED goes back to "Awaiting command...". LunaSH says:

```
Command Result : No Error
```

New, reuse, and overwrite options

The table below summarizes the steps involving Luna PED immediately after you invoke the command **hsm init**. The steps in the table are in the order in which they appear as PED prompts, descending down the column.

The first column is the simplest, and most like what you would encounter the very first time you initialize, using "fresh from the carton" PED keys.

The next two columns of the table show some differences if you are using previously-imprinted PED keys, choosing either to reuse what is found on the key (imprint it on your new HSM - see "Shared PED Key Secrets" on page 1) or, to overwrite what is found and generate a new secret to be imprinted on both the PED key and the HSM.

New PED Keys	Existing PED Keys (Reuse)	Existing PED Keys (Overwrite)
SLOT 01 SETTING SO PIN... Would you like to reuse an existing keyset? (Y/N) **No**	SLOT 01 SETTING SO PIN... Would you like to reuse an existing keyset? (Y/N) **Yes**	SLOT 01 SETTING SO PIN... Would you like to reuse an existing keyset? (Y/N) **No**

New PED Keys	Existing PED Keys (Reuse)	Existing PED Keys (Overwrite)
SLOT 01 SETTING SO PIN... Insert a SO / HSM Admin PED Key Press ENTER.	SLOT 01 SETTING SO PIN... Insert a SO / HSM Admin PED Key Press ENTER.	Slot 01 SETTING SO PIN... Insert a SO / HSM Admin PED Key Press ENTER.
This PED Key is blank. Overwrite? (YES/NO) **Yes**	****Warning!**** This PED Key is for SO / HSM Admin Overwrite? (YES/NO) **No**	****Warning!**** This PED Key is for SO / HSM Admin Overwrite? (YES/NO) **Yes**
Enter a new PED PIN Confirm new PED PIN > Press **Enter** for no PED PIN OR > Input 4-16 digits on the PED keypad and press **Enter**	Enter a new PED PIN Confirm new PED PIN > Press **Enter** for no PED PIN OR > Input 4-16 digits on the PED keypad and press **Enter**	Enter a new PED PIN Confirm new PED PIN > Press **Enter** for no PED PIN OR > Input 4-16 digits on the PED keypad and press **Enter**
Are you duplicating this keyset? YES/NO > **Yes**: duplicate. This option can be looped for as many duplicates as you need > **No**: do not duplicate	Are you duplicating this keyset? YES/NO > **Yes**: duplicate. This option can be looped for as many duplicates as you need > **No**: do not duplicate	Are you duplicating this keyset? YES/NO > **Yes**: duplicate. This option can be looped for as many duplicates as you need > **No**: do not duplicate
Login SO / HSM Admin... Insert a SO/ HSM Admin PED Key Press ENTER	Login SO / HSM Admin.. Insert a SO/ HSM Admin PED Key Press ENTER	Login SO / HSM Admin.. Insert a SO/ HSM Admin PED Key Press ENTER
SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) > **Yes** (unless you have good reason to create a new domain)	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) > **Yes**: make this HSM part of an existing domain > **No**: create a new domain for this HSM	SETTING DOMAIN... Would you like to reuse an existing keyset? (Y/N) > **Yes**: make this HSM part of an existing domain > **No**: create a new domain for this HSM

Password-authenticated HSM Initialization Example

```
lunacm:>hsm init -label myLunaHSM

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.
```

```
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Enter password for SO: ********

        Re-enter password for SO: ********

        Option -domain was not specified.  It is required.

        Enter the domain name: *********

        Re-enter the domain name: *********

Command Result : No Error
```

When activity is complete, the system displays a “success” message.

CHAPTER 2: Set the HSM Policies

SafeNet Luna HSMs are built on one of our general-purpose HSM platforms (hardware plus firmware), with a range of capabilities allowing them to be customized for specific use cases.

Some capabilities are static and cannot be changed.

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:

This section describes how to modify HSM Policies, and suggests some examples of changes best made before the HSM is further configured for use in your environment. Refer to the instructions for your HSM authentication type:

Setting SafeNet Luna PCIe HSM Policies, PW-authenticated

HSM Capabilities represent the underlying factory configurations of the HSM. HSM Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can enable a Capability. If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values.

Example Policy Change Procedure

In this example, we show the initial values of the HSM Capabilities and their corresponding Policies, then we change one Policy, and show the values again. The settings you would see for a password-authenticated HSM and a PED-authenticated HSM might differ slightly, but the general principle and the operation of policy change are the same.

1. First, for this example, display the basic HSM information.

```
lunacm:> hsm showinfo

        Partition Label -> myPCIe7hsm
        Partition Manufacturer -> SafeNet
        Partition Model -> Luna K7
        Partition Serial Number -> 528499
        Partition Status -> L3 Device
        HSM Certificates ->     *** Test Certs ***
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RNG
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
```

```
        RPV Initialized -> Not Supported
        Slot Id -> 104
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 00000000000000073100800

        Partition Storage:
                Total Storage Space:  393216
                Used Storage Space:   0
                Free Storage Space:   393216
                Object Count:         0
                Overhead:             9848

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***

        FM HW Status ->         FM
        Firmware Version -> 7.4.0
        Rollback Firmware Version -> Not Available

        Environmental:
                Fan 1 Status                          : active
                Fan 2 Status                          : failed
                Battery Voltage                       : 3.093 V
                Battery Warning Threshold Voltage     : 2.750 V
                System Temp                           : 40 deg. C
                System Temperature Warning Threshold  : 75 deg. C

        HSM Storage:
                Total Storage Space:  33554432
                Used Storage Space:   335544
                Free Storage Space:   33218888
                Allowed Partitions:   1
                Number of Partitions: 1

        License Count -> 9
                1. 621000068-000 Test Cert : K7 Base
                2. 621010185-003 Key backup via cloning protocol
                3. 621000046-002 Maximum 100 partitions
                4. 621000134-002 Enable 32 megabytes of object storage
                5. 621000135-002 Enable allow decommissioning
                6. 621000021-002 Maximum performance
                7. 621000138-001 Controlled tamper recovery
                8. 621000154-001 Enable decommission on tamper with
                   policy off
                9. 621000074-001 Test Cert : Enable Functionality
                   Modules w Policy Off

Command Result : No Error


Command Result : No Error
```

Note the message stating that the HSM is not in FIPS 140-2 approved operation mode. This is a condition that we are about to change for the purpose of providing an example; you do not need to make this particular change unless your organization's security policy calls for it.

2. Now display the controlling policies as they currently exist on the HSM.

```
lunacm:> hsm showpolicies
        HSM Capabilities
                 0: Enable PIN-based authentication : 1
                 1: Enable PED-based authentication : 0
                 2: Performance level : 15
                 4: Enable domestic mechanisms & key sizes : 1
                 6: Enable masking : 0
                 7: Enable cloning : 1
                 9: Enable full (non-backup) functionality : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
                17: Enable Korean Algorithms : 0
                18: FIPS evaluated : 0
                19: Manufacturing Token : 0
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 0
                27: HSM non-volatile storage space : 33554432
                30: Enable unmasking : 1
                33: Maximum number of partitions : 1
                35: Enable Single Domain : 0
                36: Enable Unified PED Key : 0
                37: Enable MofN : 0
                38: Enable small form factor backup/restore : 0
                39: Enable Secure Trusted Channel : 1
                40: Enable decommission on tamper : 1
                42: Enable partition re-initialize : 0
                43: Enable low level math acceleration : 1
                46: Allow Disabling Decommission : 1
                47: Enable Tunnel Slot : 0
                48: Enable Controlled Tamper Recovery : 1
                49: Enable Partition Utilization Metrics : 1
                50: Enable Functionality Modules : 1
                51: Enable SMFS Auto Activation : 1
                52: Enable Disabling FM Privilege Level : 1
                53: Enable FM Cipher Engine Key Encryption : 1

        HSM Policies
                 0: PIN-based authentication : 1
                 7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 1
                15: SO can reset partition PIN : 0
                16: Allow network replication : 1
                21: Force user PIN change after set/reset : 1
                22: Allow offboard storage : 1
                30: Allow unmasking : 1
                33: Current maximum number of partitions : 1
                39: Allow Secure Trusted Channel : 0
                40: Decommission on tamper : 0
                43: Allow low level math acceleration : 1
                46: Disable Decommission : 0
                48: Do Controlled Tamper Recovery : 1
                49: Allow Partition Utilization Metrics : 1
                50: Allow Functionality Modules : 1
                51: Allow SMFS Auto Activation : 0
```

```
                52: Disable FM Privilege Level : 0
                53: Do FM Cipher Engine Key Encryption : 0


Command Result : No Error
```

3. For this example, to change an HSM Policy setting, you must provide the number that identifies the Policy and then the value for the desired state. First login to the HSM using Luna PED (Luna PED must be connected and ready before you login). For a password-authenticated HSM the password is needed, and no PED is involved. Type the **hsm changeHSMPolicy** command:

```
lunacm:>role login -name so

        enter password: ********

Command Result : No Error

lunacm:>hsm changehsmpolicy -policy 12 -value 0

        You are about to change a destructive HSM policy.
        All partitions of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error

LunaCM v7.4.0. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->              103
        Label ->                myPCIeHSM
        Serial Number ->        123456
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PW) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device


        Current Slot Id: 103


lunacm:> hsm showpolicies
        HSM Capabilities
                 0: Enable PIN-based authentication : 1
                 1: Enable PED-based authentication : 0
                 2: Performance level : 15
                 4: Enable domestic mechanisms & key sizes : 1
                 6: Enable masking : 0
                 7: Enable cloning : 1
                 9: Enable full (non-backup) functionality : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
                17: Enable Korean Algorithms : 0
```

```
                18: FIPS evaluated : 0
                19: Manufacturing Token : 0
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 0
                27: HSM non-volatile storage space : 33554432
                30: Enable unmasking : 1
                33: Maximum number of partitions : 1
                35: Enable Single Domain : 0
                36: Enable Unified PED Key : 0
                37: Enable MofN : 0
                38: Enable small form factor backup/restore : 0
                39: Enable Secure Trusted Channel : 1
                40: Enable decommission on tamper : 1
                42: Enable partition re-initialize : 0
                43: Enable low level math acceleration : 1
                46: Allow Disabling Decommission : 1
                47: Enable Tunnel Slot : 0
                48: Enable Controlled Tamper Recovery : 1
                49: Enable Partition Utilization Metrics : 1
                50: Enable Functionality Modules : 1
                51: Enable SMFS Auto Activation : 1
                52: Enable Disabling FM Privilege Level : 1
                53: Enable FM Cipher Engine Key Encryption : 1

        HSM Policies
                 0: PIN-based authentication : 1
                 7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 0
                15: SO can reset partition PIN : 0
                16: Allow network replication : 1
                21: Force user PIN change after set/reset : 1
                22: Allow offboard storage : 1
                30: Allow unmasking : 1
                33: Current maximum number of partitions : 1
                39: Allow Secure Trusted Channel : 0
                40: Decommission on tamper : 0
                43: Allow low level math acceleration : 1
                46: Disable Decommission : 0
                48: Do Controlled Tamper Recovery : 1
                49: Allow Partition Utilization Metrics : 1
                50: Allow Functionality Modules : 1
                51: Allow SMFS Auto Activation : 0
                52: Disable FM Privilege Level : 0
                53: Do FM Cipher Engine Key Encryption : 0


Command Result : No Error



lunacm:>hsm showinfo

        Partition Label -> myPCIeHSM
        Partition Manufacturer -> Gemalto
        Partition Model -> Luna K7
        Partition Serial Number -> 123456
```

```
Partition Status -> L3 Device
HSM Part Number -> 808-000048-002
Token Flags ->
        CKF_RESTORE_KEY_NOT_NEEDED
        CKF_TOKEN_INITIALIZED
RPV Initialized -> Not Supported
Slot Id -> 103
Session State -> CKS_RW_PUBLIC_SESSION
Role Status ->   none logged in
Token Flags ->
        TOKEN_KCV_CREATED
Partition OUID: 00000000000000001b030100

Partition Storage:
        Total Storage Space:  393216
        Used Storage Space:   0
        Free Storage Space:   393216
        Object Count:         4
        Overhead:             9640

*** The HSM is in FIPS 140-2 approved operation mode. ***
```

Note in the above example that HSM Capability "12: Enable non-FIPS algorithms : 1" still has a value of 1 (meaning that it remains enabled), but the associated Policy "12: Allow non-FIPS algorithm : **0** " now has a value of 0 (meaning that it has been disallowed by the SO).

Note also that the message in the middle of the "show" information now says "*** The HSM is in FIPS 140-2 approved operation mode. *** " because the HSM is now restricted to using only FIPS-approved algorithms.

Destructive Change of HSM Policy

The above example is a change to a destructive policy. This means that if you apply this policy, the HSM is zeroized and all contents are lost. For this reason, you are prompted to confirm if that is what you really wish to do. You must now re-initialize the HSM.

While this is not an issue when you have just initialized an HSM, it may be a very important consideration if your SafeNet Luna HSM has been in a “live” or “production” environment and contains useful or important data, keys, certificates.

Backup any important HSM or partition contents before making any destructive policy change, and then restore from backup after the HSM is re-initialized and the partition re-created.

Refer to "Capabilities and Policies" on page 1 in the *HSM Administration Guide* for a description of all policies and their meanings.

Setting SafeNet Luna PCIe HSM Policies, PED-authenticated

HSM Capabilities represent the underlying factory configurations of the HSM. HSM Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can enable a Capability. If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values.

Example Policy Change Procedure

In this example, we show the initial values of the HSM Capabilities and their corresponding Policies, then we change one Policy, and show the values again. The settings you would see for a password-authenticated HSM and a PED-authenticated HSM might differ slightly, but the general principle and the operation of policy change are the same.

1. First, for this example, display the basic HSM information.

```
lunacm:>hsm showinfo

        Partition Label -> myPCIeHSM
        Partition Manufacturer -> Gemalto
        Partition Model -> Luna K7
        Partition Serial Number -> 123456
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> No
        Slot Id -> 103
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 00000000000000001b030100

        Partition Storage:
                Total Storage Space:  393216
                Used Storage Space:   0
                Free Storage Space:   393216
                Object Count:         4
                Overhead:             9640

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***

        Firmware Version -> 7.0.1
        Rollback Firmware Version -> Not Available

        Environmental:
                Fan 1 Status                          : active
                Fan 2 Status                          : active
                Battery Voltage                       : 3.093 V
                Battery Warning Threshold Voltage     : 2.750 V
                System Temp                           : 34 deg. C
                System Temperature Warning Threshold  : 75 deg. C
        HSM Storage:
                Total Storage Space:  33554432
                Used Storage Space:   0
                Free Storage Space:   33554432
                Allowed Partitions:   100
                Number of Partitions: 0

        License Count -> 8
                1. 621000153-000 K7 base configuration
                2. 621010185-003 Key backup via cloning protocol
```

```
                3. 621000046-002 Maximum 100 partitions
                4. 621000134-002 Enable 32 megabytes of object storage
                5. 621000135-002 Enable allow decommissioning
                6. 621000021-002 Maximum performance
                7. 621000138-001 Controlled tamper recovery
                8. 621000154-001 Enable decommission on tamper with policy off
                9. 621000145-002 Enable PED authentication with M of N
                10. 621010089-002 Enable remote PED capability

Command Result : No Error
```

Note the message stating that the HSM is not in FIPS 140-2 approved operation mode. This is a condition that we are about to change for the purpose of providing an example; you do not need to make this particular change unless your organization's security policy calls for it.

2. Now display the controlling policies as they currently exist on the HSM.

```
lunacm:>hsm showpolicies

        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                2: Performance level : 15
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 0
                7: Enable cloning : 1
                9: Enable full (non-backup) functionality : 1
               12: Enable non-FIPS algorithms : 1
               15: Enable SO reset of partition PIN : 1
               16: Enable network replication : 1
               17: Enable Korean Algorithms : 0
               18: FIPS evaluated : 0
               19: Manufacturing Token : 0
               21: Enable forcing user PIN change : 1
               22: Enable offboard storage : 1
               23: Enable partition groups : 0
               25: Enable remote PED usage : 1
               27: HSM non-volatile storage space : 33554432
               30: Enable unmasking : 1
               33: Maximum number of partitions : 100
               35: Enable Single Domain : 0
               36: Enable Unified PED Key : 0
               37: Enable MofN : 0
               38: Enable small form factor backup/restore : 0
               39: Enable Secure Trusted Channel : 1
               40: Enable decommission on tamper : 1
               42: Enable partition re-initialize : 0
               43: Enable low level math acceleration : 1
               45: Enable Fast-Path : 0
               46: Allow Disabling Decommission : 1
               47: Enable Tunnel Slot : 0
               48: Enable Controlled Tamper Recovery : 1

        HSM Policies
                0: PIN-based authentication : 0
                1: PED-based authentication : 1
                6: Allow masking : 0
                7: Allow cloning : 1
               12: Allow non-FIPS algorithms : 1
               15: SO can reset partition PIN : 0
               16: Allow network replication : 1
               21: Force user PIN change after set/reset : 1
```

```
                22: Allow offboard storage : 1
                23: Allow partition groups : 0
                25: Allow remote PED usage : 1
                30: Allow unmasking : 1
                33: Current maximum number of partitions : 100
                35: Force Single Domain : 0
                36: Allow Unified PED Key : 0
                37: Allow MofN : 0
                38: Allow small form factor backup/restore : 0
                39: Allow Secure Trusted Channel : 0
                40: Decommission on tamper : 0
                42: Allow partition re-initialize : 0
                43: Allow low level math acceleration : 1
                45: Allow Fast-Path : 0
                46: Disable Decommission : 0
                47: Allow Tunnel Slot : 0
                48: Do Controlled Tamper Recovery : 1

Command Result : No Error
```

3. For this example, to change an HSM Policy setting, you must provide the number that identifies the Policy and then the value for the desired state. First login to the HSM using Luna PED (Luna PED must be connected and ready before you login). For a password-authenticated HSM the password is needed, and no PED is involved). Type the **hsm changeHSMPolicy** command:

```
lunacm:>role login -name so

        Please attend to the PED.
```

> **NOTE** At this time, you must respond to the prompts on the Luna PED screen.

```
Command Result : No Error


lunacm:>hsm changehsmpolicy -policy 12 -value 0

        You are about to change a destructive HSM policy.
        All partitions of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error

LunaCM v7.0.0. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->              103
        Label ->                myPCIeHSM
        Serial Number ->        123456
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           L3 Device
```

```
        Current Slot Id: 103


lunacm:>hsm showpolicies

        HSM Capabilities
                 0: Enable PIN-based authentication : 0
                 1: Enable PED-based authentication : 1
                 2: Performance level : 15
                 4: Enable domestic mechanisms & key sizes : 1
                 6: Enable masking : 0
                 7: Enable cloning : 1
                 9: Enable full (non-backup) functionality : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
                17: Enable Korean Algorithms : 0
                18: FIPS evaluated : 0
                19: Manufacturing Token : 0
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 1
                27: HSM non-volatile storage space : 33554432
                30: Enable unmasking : 1
                33: Maximum number of partitions : 100
                35: Enable Single Domain : 0
                36: Enable Unified PED Key : 0
                37: Enable MofN : 0
                38: Enable small form factor backup/restore : 0
                39: Enable Secure Trusted Channel : 1
                40: Enable decommission on tamper : 1
                42: Enable partition re-initialize : 0
                43: Enable low level math acceleration : 1
                45: Enable Fast-Path : 0
                46: Allow Disabling Decommission : 1
                47: Enable Tunnel Slot : 0
                48: Enable Controlled Tamper Recovery : 1

        HSM Policies
                 0: PIN-based authentication : 0
                 1: PED-based authentication : 1
                 6: Allow masking : 0
                 7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 0
                15: SO can reset partition PIN : 0
                16: Allow network replication : 1
                21: Force user PIN change after set/reset : 1
                22: Allow offboard storage : 1
                23: Allow partition groups : 0
                25: Allow remote PED usage : 1
                30: Allow unmasking : 1
                33: Current maximum number of partitions : 100
                35: Force Single Domain : 0
                36: Allow Unified PED Key : 0
                37: Allow MofN : 0
                38: Allow small form factor backup/restore : 0
                39: Allow Secure Trusted Channel : 0
                40: Decommission on tamper : 0
                42: Allow partition re-initialize : 0
                43: Allow low level math acceleration : 1
```

```
                45: Allow Fast-Path : 0
                46: Disable Decommission : 0
                47: Allow Tunnel Slot : 0
                48: Do Controlled Tamper Recovery : 1

Command Result : No Error


lunacm:>hsm showinfo

        Partition Label -> myLunaHSM
        Partition Manufacturer -> Gemalto
        Partition Model -> Luna K7
        Partition Serial Number -> 532018
        Partition Status -> L3 Device
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> Not Supported
        Slot Id -> 103
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 00000000000000001b030100

        Partition Storage:
                Total Storage Space:  393216
                Used Storage Space:   0
                Free Storage Space:   393216
                Object Count:         4
                Overhead:             9640

        *** The HSM is in FIPS 140-2 approved operation mode. ***
```

Note in the above example that HSM Capability "12: Enable non-FIPS algorithms : 1" still has a value of 1 (meaning that it remains enabled), but the associated Policy "12: Allow non-FIPS algorithm : **0** " now has a value of 0 (meaning that it has been disallowed by the SO).

Note also that the message in the middle of the "show" information now says "*** The HSM is in FIPS 140-2 approved operation mode. *** " because the HSM is now restricted to using only FIPS-approved algorithms.

Destructive Change of HSM Policy

The above example is a change to a destructive policy. This means that if you apply this policy, the HSM is zeroized and all contents are lost. For this reason, you are prompted to confirm if that is what you really wish to do. You must now re-initialize the HSM.

While this is not an issue when you have just initialized an HSM, it may be a very important consideration if your SafeNet Luna HSM has been in a “live” or “production” environment and contains useful or important data, keys, certificates.

Backup any important HSM or partition contents before making any destructive policy change, and then restore from backup after the HSM is re-initialized and the partition re-created.

CHAPTER 3: Creating an Application Partition on the HSM

In a previous chapter, you initialized the HSM, establishing ownership and administrative oversight by the HSM Security Officer, using the authentication method that is supported by your HSM (password-authenticated or PED-authenticated). In this chapter, you establish a separate space in the HSM for use by your cryptographic applications - for creation, storage, and use of cryptographic keys and objects.

The set of instructions that apply to your HSM and application partition depends on the type of authentication used by your HSM, and therefore by any application partitions (which was decided when you purchased the HSM), as follows:

> "Configure a Password-Authenticated Application Partition" below

> "Configuring a PED-Authenticated Application Partition" on page 36

Configure a Password-Authenticated Application Partition

You have already initialized and configured your password-authenticated SafeNet Luna PCIe HSM, to the point of initializing the HSM and assigning a Security Officer to administer it, as well as setting any HSM-wide configuration options. In this chapter, you will create and configure an application partition on your password-authenticated HSM. The partition you create has its own Security Officer and is largely invisible to the HSM SO.

High-Level Configuration Steps

1. "HSM SO Creates Password-Authenticated Partition, Local to Client" below
2. "Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition" on page 34
3. "Initialize the Crypto User Role on a PW-Authenticated Partition" on page 35

HSM SO Creates Password-Authenticated Partition, Local to Client

An application owner/user has requested an application partition on the HSM, on which applications will run cryptographic operations. These instructions are the actions to be taken by the HSM SO. These instructions assume a Password-authenticated SafeNet Luna PCIe HSM.

These instructions assume an HSM installed locally to the host computer, where SafeNet Luna HSM Client software is installed, and where administrative access to the HSM is carried out via the LunaCM tool.

Verification

These instructions assume that the HSM is new, or has undergone factory reset and is in zeroized state with no HSM SO or Administrator role set. This can be verified by running the LunaCM command **hsm showinfo** while the HSM is the selected cryptographic slot. For example:

```
lunacm:>slot list

        Slot Id ->              103
        Label ->
        Serial Number ->        66331
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PW) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device, Zeroized


        Current Slot Id: 4

Command Result : No Error
```

The output shows that the host computer contains a password-authenticated SafeNet Luna PCIe HSM at the desired firmware version, as slot 103. The SafeNet Luna PCIe HSM admin partition is the currently-set slot, so all commands are directed to that HSM. When new partitions are created, or other SafeNet Luna HSMs are attached, you will need to select their slots using the LunaCM command **slot set** to direct commands to them.

```
lunacm:>hsm showinfo

        Partition Label ->
        Partition Manufacturer -> Gemalto
        Partition Model -> Luna K7
        Partition Serial Number -> 66331
        Partition Status -> L3 Device, Zeroized
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
        RPV Initialized -> Not Supported
        Slot Id -> 103
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
```

The HSM in the current slot is zeroized and ready to be configured.

Configuration

1. Initialize the HSM.

   hsm init -label <label>

   PKCS slot numbering starts at zero. A slot zero (0) always exists, as a placeholder for partitions to be created. For consistency in operation, the HSM administrative partition must always be the highest-numbered slot on that HSM. The admin partition's slot number will depend on the number of possible partitions that can be created on your model of HSM.

2. List the slots to see that the HSM is no longer zeroized.

   slot list

```
lunacm:>slot list

        Slot Id ->              4
        Label ->                myPCIeHSM
        Serial Number ->        66331
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PW) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device


        Current Slot Id: 4


Command Result : No Error
```

3. Log in as the HSM Security Officer:

   role login -name SO

4. Create an application partition. You can specify a slot to be used for the current session by specifying the **-slot** option. Slots will be reordered the next time you restart LunaCM. Note that the HSM administrative partition is always the highest-numbered slot.

   partition create

5. Verify the slot occupied by the new, empty, application partition, and check the currently active slot.

   slot list

```
lunacm:>slot list

        Slot Id ->              3
        Label ->
        Serial Number ->        154438865289
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                myPCIeHSM
        Serial Number ->        66331
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PW) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PW)
        HSM Status ->           L3 Device


        Current Slot Id: 4

Command Result : No Error
```

6. The HSM SO now informs the intended Partition SO:

   a. The newly created, empty application partition is ready

b. How to access the partition

This concludes the HSM SO's actions for a partition. Further action in the new partition must be initiated by the Partition SO, who takes over responsibility as the chief authority of that partition. The HSM SO has no visibility into the new partition.

Go to "Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition" below.

Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition

These instructions assume a password-authenticated SafeNet Luna PCIe HSM has been initialized, and an application partition has been created (see previous steps by HSM SO "HSM SO Creates Password-Authenticated Partition, Local to Client" on page 31).

Label, Domain, and Password Rules

The partition label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>`~
```

Question marks (`?`) and double quotation marks (`"`) are not allowed.

Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

The domain string must be 1-128 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^*-_=+[]{}/:',.~
```

The following characters are problematic or invalid and must not be used in a domain string: `"&;<>\`|()`

Spaces are allowed, as long as the leading character is not a space; to specify a domain string with spaces using the **-domain** option, enclose the string in double quotation marks.

In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>?`~
```

Double quotation marks (`"`) are problematic and should not be used in passwords.

Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

For more information, refer to "Name, Label, and Password Requirements" on page 1.

To initialize the Partition SO and Crypto Officer roles:

Step 1: Initialize the Partition SO role

1. Set the active slot to the uninitialized application partition:

   lunacm:>**slot set -slot** <slotnum>

2. Initialize the application partition, to create the partition's Security Officer (SO), and set the initial password and cloning domain.

   lunacm:>**partition init -label** <par_label>

Step 2: Initialize the Crypto Officer role

The SO of the application partition can now assign the first operational role within the new partition.

1. First, login as Partition SO. You can also use the shortcut **po**.

   role login -name Partition SO

2. Initialize the Crypto Officer role and set the initial password. You can also use the shortcut **co**.

   role init -name Crypto Officer

3. he Partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, you must log out to allow the Crypto Officer to log in with the newly-set password.

   role logout

> **NOTE** If HSM policy **21: Force user PIN change after set/reset** is set to **1** (the default setting), the Crypto Officer must change the initial CO credential before using the partition for cryptographic operations. This applies to the activation challenge secret as well (see "role changepw" on page 1 in the *LunaCM Command Reference Guide*).

Once the Crypto Officer logs in and changes the initial credential set by the Partition SO, applications using the CO's challenge secret/password can perform cryptographic operations in the partition. The Crypto Officer can create, modify and delete crypto objects within the partition, and use existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them. The separation of roles is important in some security regimes and operational situations, and where you might be required to satisfy audit criteria for industry or government oversight.

The next sequence of configuration actions is performed by the Crypto Officer, just created for the application partition. See "Initialize the Crypto User Role on a PW-Authenticated Partition" below.

Initialize the Crypto User Role on a PW-Authenticated Partition

These instructions assume:

- A password-authenticated SafeNet Luna PCIe HSM has been initialized
- An application partition has been created
- A Crypto Officer has been created for the partition
- The Crypto Officer password has been conveyed to the person responsible for the Crypto Officer role. See "Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition" on the previous page.

As Crypto Officer, you can:

- Create a Crypto User (limited access user) for the application partition.
- Create, delete, change and manipulate cryptographic objects on the application partition, either for your own use or for use by the Crypto User.

To initialize the Crypto User role

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.

   lunacm:>**slot set -slot** <slotnum>

2. Log in as the Crypto Officer. You can also use the shortcut **co**.

   lunacm:>**role login -name Crypto Officer**

   > **NOTE** The password for the Crypto Officer role is valid for the initial login only. You must change the initial password using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED error when you perform role-dependent actions.

3. If you have not already done so, change the initial password set by the Partition SO.

   In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:
   `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>?`~`
   Double quotation marks (") are problematic and should not be used in passwords.
   Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

   lunacm:>**role changepw -name co**

4. Create the Crypto User. You can also use the shortcut **cu**.

   lunacm:>**role init -name Crypto User**

   > **NOTE** The password for the Crypto User role is valid for the initial login only. The CU must change the initial password using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED error when they perform role-dependent actions.

The Crypto User can now login with the credentials provided by the Crypto Officer, and change the initial password. The Crypto User can now use applications to perform cryptographic operations using keys and objects created in the partition by the Crypto Officer.

Configuring a PED-Authenticated Application Partition

You have already initialized and configured your PED-authenticated SafeNet Luna PCIe HSM, to the point of initializing the HSM and assigning a Security Officer to administer it, as well as setting any HSM-wide configuration options. In this chapter, you will create and configure an application partition on your PED-authenticated HSM. The partition you create has its own separate Security Officer and is largely invisible to the HSM SO.

High-Level Configuration Steps

1. "HSM SO Creates PED-Authenticated Partition, Local to Client" on the next page
2. "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition" on page 39
3. "Initialize the Crypto User Role on a PW-Authenticated Partition" on the previous page
4. [Optional] Activate the Crypto Officer and/or Crypto User roles. See "Activate a PED-Authenticated Partition" on page 42.

HSM SO Creates PED-Authenticated Partition, Local to Client

An application owner/user has requested an application partition on the HSM, on which applications will run cryptographic operations. These instructions are the actions to be taken by the HSM SO. These instructions assume a PED-authenticated SafeNet Luna PCIe HSM.

These instructions assume an HSM installed locally to the host computer, where SafeNet Luna HSM Client software is installed, and where administrative access to the HSM is carried out via the LunaCM utility.

Requirements

You will need:

> A Luna PED and PED keys with labels and a locally-connected PED.

Verification

These instructions assume that the HSM is new, or has undergone factory reset and is in zeroized state with no HSM SO or Administrator role set. This can be verified by running the lunacm command **hsm showinfo** while the HSM is the selected cryptographic slot. For example:

```
lunacm:>slot list

        Slot Id ->              4
        Label ->
        Serial Number ->        532018
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           L3 Device, Zeroized


        Current Slot Id: 103


Command Result : No Error
```

The output shows that the host computer contains a PED-authenticated SafeNet Luna PCIe HSM at the desired firmware version, as slot 103. The SafeNet Luna PCIe HSM admin partition is the currently-set slot, so all commands are directed to that HSM. When new partitions are created, or other SafeNet Luna HSMs are attached, you will need to select their slots using the LunaCM command **slot set** to direct commands to them.

```
lunacm:>hsm showinfo

        Partition Label ->
        Partition Manufacturer -> SafeNet
        Partition Model -> Luna K7
        Partition Serial Number -> 532018
        Partition Status -> L3 Device, Zeroized
        HSM Part Number -> 808-000048-002
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        RPV Initialized -> No
        Slot Id -> 4
```

```
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->
```

The HSM in the current slot is zeroized and ready to be configured.

Configuration

Have a blue HSM SO PED key and a red Domain PED key ready, and have a Luna PED connected to the HSM, set to Local Mode.

1. Initialize the HSM.

   hsm init -label <label>

   Respond to Luna PED prompts...

   PKCS slot numbering starts at zero. A slot zero (0) always exists, as a placeholder for partitions to be created. For consistency in operation, the HSM administrative partition must always be the highest-numbered slot on that HSM. The admin partition's slot number will depend on the number of possible partitions that can be created on your model of HSM.

2. List the slots to see that the HSM is no longer zeroized.

   slot list

```
lunacm:>slot list

        Slot Id ->              4
        Label ->                myPCIeHSM
        Serial Number ->        532018
        Model ->                Luna K7
        Firmware Version ->     7.0.1
        Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           L3 Device


        Current Slot Id: 103


Command Result : No Error
```

3. Log in as the HSM Security Officer.

   role login -name SO

   Respond to Luna PED prompts...

4. Create an application partition. You can specify a slot to be used for the current session by specifying the **-slot** option. Slots will be reordered the next time you restart LunaCM. Note that the HSM administrative partition is always the highest-numbered slot.

   partition create

5. Verify the slot occupied by the new, empty, application partition, and check the currently active slot.

   slot list

6. The HSM SO now informs the intended Partition SO:

   a. The newly created, empty application partition is ready

b. How to access the partition

This concludes the HSM SO's actions for a partition. Further action in the new partition must be initiated by the Partition SO, who takes over responsibility as the chief authority of that partition. The HSM SO has no visibility into the new partition.

Go to "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition" below.

Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition

These instructions assume a PED-authenticated SafeNet Luna PCIe HSM has been initialized, and an application partition has been created.

You will need:

These instructions assume that you have already made your decisions whether to use all-new, blank PED keys, or to re-use any existing, imprinted PED keys for any of the steps.

To initialize the Partition SO and Crypto Officer roles:

Step 1: Initialize the Partition SO role

Have a blue HSM SO PED key and a red Domain PED key ready.

1. Set the active slot to the uninitialized application partition:

   lunacm:>**slot set -slot** <slotnum>

2. Initialize the application partition, to create the partition's blue Security Officer (SO) PED key and the red cloning domain PED key.

   The partition label created during initialization must be 1-32 characters in length. If you specify a longer label, it will automatically be truncated to 32 characters. The following characters are allowed:
   `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>`~`
   Question marks (`?`) and double quotation marks (`"`) are not allowed.
   Spaces are allowed; enclose the label in double quotation marks if it includes spaces.

   lunacm:>**partition init -label** <par_label>

   Respond to Luna PED prompts...

Step 2: Initialize the Crypto Officer role

The SO of the application partition can now assign the first operational role within the new partition. Have a black Crypto Officer PED key ready.

1. First, login as Partition SO. You can also use the shortcut **po**.

   lunacm:>**role login -name Partition SO**

2. Initialize the Crypto Officer role. You can also use the shortcut **co**.

   lunacm:>**role init -name Crypto Officer**

   Respond to Luna PED prompts...

3. The Partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, you must log out to allow the Crypto Officer to log in.

   lunacm:>**role logout**

> **NOTE** If HSM policy **21: Force user PIN change after set/reset** is set to **1** (the default setting), the Crypto Officer must change the initial CO credential before using the partition for cryptographic operations. This applies to the activation challenge secret as well (see "role changepw" on page 1 in the *LunaCM Command Reference Guide*).

Step 3 (OPTIONAL): Enable Partition activation

Activation allows the Crypto Officer/User PED credentials to be cached when the role logs in, and open and close subsequent sessions using a challenge secret (password). To activate the partition, follow the steps for the "Partition SO" on page 42.

For more about activation, see "Activation and Auto-activation on PED-Authenticated Partitions" on page 1 in the *Administration Guide*.

Once the Crypto Officer logs in and changes the initial credential set by the Partition SO, applications using the CO's challenge secret/password can perform cryptographic operations in the partition. The Crypto Officer can create, modify and delete crypto objects within the partition, and use existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them. The separation of roles is important in some security regimes and operational situations, and where you might be required to satisfy audit criteria for industry or government oversight.

The next sequence of configuration actions is performed by the Crypto Officer, just now created for the application partition. See "Initialize the Crypto User Role on a PED-Authenticated Partition" below.

Initialize the Crypto User Role on a PED-Authenticated Partition

These instructions assume:

- A PED-authenticated SafeNet Luna PCIe HSM has been initialized
- An application partition has been created
- A Crypto Officer has been created for the partition
- The Crypto Officer PED key has been conveyed to the person responsible for the Crypto Officer role. See "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition" on the previous page.

As Crypto Officer, you can:

- Create a Crypto User (limited access user) for the application partition.
- Create, delete, change and manipulate cryptographic objects on the application partition, either for your own use or for use by the Crypto User.
- Activate the partition for use by applications.

To create a Crypto User for the partition, you will need:

- Luna PED and the black Crypto Officer PED key(s) assigned to you by the SO.
- Blank PED key(s) with labels for the Crypto User that you are about to create.
- A local PED connection.

These instructions assume that you have already made your decisions whether to use all-new, blank PED keys, or to re-use any existing, imprinted PED keys for any of the steps.

To create the Crypto User role on a PED-authenticated application partition:

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.

   lunacm:> **slot set -slot** <slotnum>

2. Log in as the Crypto Officer. You can also use the shortcut **co**.

   lunacm:>**role login -name Crypto Officer**

   Respond to Luna PED prompts...

   > **NOTE** The black Crypto Officer PED key is valid for the initial login only. You must change the initial credential on the key using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_ EXPIRED error when you perform role-dependent actions.

3. If you have not already done so, change the initial credential set by the Partition SO.

   lunacm:>**role changepw -name Crypto Officer**

   Respond to Luna PED prompts. You must first present the black Crypto Officer key and PIN created by the Partition SO. When you are prompted to present a new black CO key, you can create a new key, or overwrite the original PED key by:

   a. Replying **No** to "Would you like to reuse an existing keyset?"

   b. Pressing **Enter** (without removing the key) when prompted to present a new black PED key

   c. Replying **Yes** when asked if you want to overwrite the original key.

4. Create the Crypto User. You can also use the shortcut **cu**. Have a gray Crypto User PED key ready.

   role init -name Crypto User

   Respond to Luna PED prompts...

   > **NOTE** The gray Crypto User PED key is valid for the initial login only. The CU must change the initial credential on the key using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_ EXPIRED error when they perform role-dependent actions.

The Crypto User can now log in to use applications to perform cryptographic operations using keys and objects created in the partition by the Crypto Officer.

Crypto Officer or Crypto User Must Remain Logged In

At this point, the Crypto User, or an application using the CU's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto User logs in with **role login -name cu**. However, any event that causes that session to close, including action by the application, requires that the CU must log in again (with the gray PED key) before the application partition can be used again. For an application

that maintains an open session, that is not a handicap. For an application that opens a session for each action, performs the cryptographic action, then closes the session, the CU must be constantly logging in and using the PED and PED key.

To bypass this limitation, use the Activation feature. See "Activate a PED-Authenticated Partition" below.

Activate a PED-Authenticated Partition

In this section, the Partition SO configures the partition to allow Activation (caching of the authentication credential). Once the Activation policy is set, credentials are cached the next time the Crypto Officer or Crypto User logs in. This allows the Crypto Officer or Crypto User to log in once using their PED key, and open and close subsequent sessions using only a challenge secret (password). The Partition SO can optionally allow Auto-Activation, which preserves the cached PED credentials in the event of a restart or a brief power outage (up to 2 hours). For more information, see "Activation and Auto-activation on PED-Authenticated Partitions" on page 1 in the *Administration Guide*.

The Partition SO must set an initial challenge secret for the Crypto Officer, and the Crypto Officer must set one for the Crypto User. See the correct section below for your user role:

> "Partition SO" below

> "Crypto Officer" on the next page

> "Crypto User [Optional]" on page 44

Partition SO

These instructions are for the Partition SO. They assume that:

> You are running LunaCM on a SafeNet Luna HSM Client host computer containing, or connected to, an HSM with an application partition.

> The partition has at least a Crypto Officer role initialized. If the Crypto User role is also initialized, activation will be enabled for both roles.

To enable activation of a PED-authenticated application partition:

1. Set the active slot to the desired application partition.

   lunacm:>**slot set -slot** <slotnum>

2. Log in as the Partition Security Officer.

   lunacm:>**role login -name po**

3. Set **partition policy 22: Allow activation** for the partition.

   lunacm:>**partition changepolicy -policy 22 -value 1**

4. [Optional] Set **partition policy 23: Allow auto-activation** for the partition.

   lunacm:>**partition changepolicy -policy 23 -value 1**

5. Create an initial challenge secret for the Crypto Officer.

   In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:

   `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>?`~`

Double quotation marks (") are problematic and should not be used in passwords.
Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

lunacm:>**role createchallenge -name co**

6. Provide the initial challenge secret to the Crypto Officer by secure means. The CO will need to change the challenge secret before using the partition for any crypto operations.
7. Log out as Partition SO.

   lunacm:>**role logout**

Once policy 22 is set, the black CO PED key credential will be cached the next time the CO logs in. From that point on, only the CO partition challenge secret is required to access the partition. The CO credential remains cached until the HSM loses power, or the role is explicitly deactivated using the command **role deactivate**. The credential is re-cached the next time the CO logs in.

> **NOTE** The Partition SO can stop automatic caching of the CO and CU credentials at any time by disabling **partition policy 22: Allow activation** (setting its value to 0).

Crypto Officer

These instructions are for the Crypto Officer. Ensure that you have the initial challenge secret password provided by the Partition SO.

To activate the Crypto Officer role on an application partition:

1. Login to the partition as the Crypto Officer. When prompted, enter the initial challenge secret.

   lunacm:>**role login -name co**

   The Crypto Officer PED secret is cached, and the role is now activated.
2. If you have not already done so on a previous login, change the initial CO PED secret. By default, the PED secret provided by the Partition SO expires after the initial login. If **HSM policy 21: Force user PIN change after set/reset** is set to **0** (off), you can continue to use the PED secret provided.

   lunacm:>**role changepw -name co**
3. Change the initial CO challenge secret. You must include the **-oldpw** option to indicate that you wish to change the challenge secret (referred to as the secondary credential), rather than the black PED key (primary credential).

   In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:
   `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>?`~`
   Double quotation marks (") are problematic and should not be used in passwords.
   Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

   lunacm:>**role changepw -name co -oldpw** <initial_challenge> **-newpw** <new_challenge>
4. [Optional] Create an initial challenge secret for the Crypto User.

   In LunaCM, passwords and challenge secrets must be 7-255 characters in length. The following characters are allowed:
   `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 !@#$%^&*()-_=+[]{}\|/;:',.<>?`~`

Double quotation marks (") are problematic and should not be used in passwords.
Spaces are allowed; to specify a password with spaces using the **-password** option, enclose the password in double quotation marks.

lunacm:>**role createchallenge -name cu**

5. [Optional] Provide the initial challenge secret to the Crypto User by secure means. The CU will need to change the challenge secret before using the partition for any crypto operations.
6. Log out as Crypto Officer.

   lunacm:>**role logout**

With activation in place, you can log in once and put your black CO PED key away in a safe place. The cached credentials will allow your application(s) to open and close sessions and perform their operations within those sessions.

Crypto User [Optional]

These instructions are for the Crypto User. Ensure that you have the initial challenge secret password provided by the Crypto Officer.

To activate the Crypto User role on an application partition:

1. Login to the partition as the Crypto User. When prompted, enter the initial challenge secret.

   lunacm:>**role login -name cu**

2. Change the initial CU challenge secret. You must include the **-oldpw** option to indicate that you wish to change the challenge secret (referred to as the secondary credential), rather than the gray PED key (primary credential).

   lunacm:>**role changepw -name cu -oldpw** <initial_challenge> **-newpw** <new_challenge>

With activation in place, you can log in once and put your gray CO PED key away in a safe place. The cached credentials will allow your application(s) to open and close sessions and perform their operations within those sessions.

CHAPTER 4: Setting SafeNet Luna PCIe HSM Partition Policies

Partition Capabilities represent the underlying factory configurations that are in force when a Partition is created. Partition Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can change a Capability from off to on (disabled to enabled). If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

For example, if a Capability setting requires that the minimum length of a Partition Password must be (say) seven characters, then the SO can use a Policy change to require a minimum password length of eight, nine, ten, or more characters (up to 255). A requirement for a longer password is considered to be a more restrictive security setting. The SO cannot use a Policy change to set the minimum password length to six or fewer characters, because that would be less restrictive than the original Capability, which demands at least seven characters.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values, as in the example below.

In this example, we will change the maximum number of consecutive failed login attempts that is permitted on the Partition before it is zeroized. The default maximum is 10. You can change the maximum to less than 10, but not more than 10. Setting to less than ten would make the partition more secure than the default, and is allowed. Setting to more than ten would make the partition less secure than the default, and is not allowed.

To change a partition policy:

1. View the current Partition Capabilities and their corresponding Policies.

   slot set slot <slotnum>

   partition showpolicies

```
lunacm:>partition showpolicies
        Partition Capabilities
                0: Enable private key cloning : 1
                1: Enable private key wrapping : 0
                2: Enable private key unwrapping : 1
                3: Enable private key masking : 0
                4: Enable secret key cloning : 1
                5: Enable secret key wrapping : 1
                6: Enable secret key unwrapping : 1
                7: Enable secret key masking : 0
               10: Enable multipurpose keys : 1
               11: Enable changing key attributes : 1
               15: Allow failed challenge responses : 1
               16: Enable operation without RSA blinding : 1
               17: Enable signing with non-local keys : 1
               18: Enable raw RSA operations : 1
               20: Max failed user logins allowed : 10
               21: Enable high availability recovery : 1
```

```
              22: Enable activation : 0
              23: Enable auto-activation : 0
              25: Minimum pin length (inverted: 255 - min) : 248
              26: Maximum pin length : 255
              28: Enable Key Management Functions : 1
              29: Enable RSA signing without confirmation : 1
              31: Enable private key unmasking : 1
              32: Enable secret key unmasking : 1
              33: Enable RSA PKCS mechanism : 1
              34: Enable CBC-PAD (un)wrap keys of any size : 1
              35: Enable private key SFF backup/restore : 0
              36: Enable secret key SFF backup/restore : 0
              37: Enable Secure Trusted Channel : 1
              38: Enable  Fast-Path : 0
              39: Enable  Start/End Date Attributes : 1

       Partition Policies
               0: Allow private key cloning : 1
               1: Allow private key wrapping : 0
               2: Allow private key unwrapping : 1
               3: Allow private key masking : 0
               4: Allow secret key cloning : 1
               5: Allow secret key wrapping : 1
               6: Allow secret key unwrapping : 1
               7: Allow secret key masking : 0
              10: Allow multipurpose keys : 1
              11: Allow changing key attributes : 1
              15: Ignore failed challenge responses : 1
              16: Operate without RSA blinding : 1
              17: Allow signing with non-local keys : 1
              18: Allow raw RSA operations : 1
              20: Max failed user logins allowed : 10
              21: Allow high availability recovery : 1
              22: Allow activation : 0
              23: Allow auto-activation : 0
              25: Minimum pin length (inverted: 255 - min) : 248
              26: Maximum pin length : 255
              28: Allow Key Management Functions : 1
              29: Perform RSA signing without confirmation : 1
              31: Allow private key unmasking : 1
              32: Allow secret key unmasking : 1
              33: Allow RSA PKCS mechanism : 1
              34: Allow CBC-PAD (un)wrap keys of any size : 1
              35: Allow private key SFF backup/restore : 0
              36: Allow secret key SFF backup/restore : 0
              37: Force Secure Trusted Channel : 0
              38: Allow Fast-Path : 0
              39: Allow Start/End Date Attributes : 0


   Command Result : No Error
```

2. Login as Partition SO.

   role login -name po

3. Use the following command to change partition policy 20's value to **5**:

   partition changepolicy -policy 20 -value 5

```
lunacm:>partition changepolicy -policy 20 -value 5

Command Result : No Error
```

4. View the partition policies again to see the change.

   partition showpolicies

```
lunacm:>partition showpolicies
        Partition Capabilities
                ...
                20: Max failed user logins allowed : 10
                ...
        Partition Policies
                ...
                20: Max failed user logins allowed : 5
                ...


Command Result : No Error
```

Note that **Partition Capability 20: Max failed user logins allowed** still has a value of 10, but the associated **Policy 20: Max failed user logins allowed** now has a value of 5 - meaning that the Partition SO has decided that 10 bad login attempts on the partition was too many. The SO has used the Policy to impose greater restriction than the Capability required, increasing security on the partition.

CHAPTER 5: Optional Configuration Tasks

After completing the base configuration, you can also perform any of the following optional configuration tasks:

Configure multiple HSMs to operate in high-availability (HA) mode

High Availability (HA) mode allows you to automatically replicate the data on a HSM/partition over two or more physical HSMs to provide redundancy and load balancing. Applications using an HA HSM/partition do not access it directly. Instead, the HA software creates a virtual slot for the partition and manages which physical HSM is actually used when responding to an application request. See "High-Availability Groups" on page 1 in the *Administration Guide*.

Configure SNMP

You can use the SNMP MIB to monitor the performance of your HSMs. See "SNMP Monitoring" on page 1 in the *Administration Guide*.

Configure a remote PED

If you are configuring a PED-authenticated HSM, you can configure it to use a remote PED, which allows you to authenticate to the HSM from a remote location. See "Remote PED Setup" on page 1 in the *Administration Guide*.

CHAPTER 6: Confirming the HSM's Authenticity

Hardware Security Modules have traditionally been deployed in the corporate data center's most secure zone. Establishing trust with the HSM is, in part, achieved by physical access control. In cases of remote client usage (such as cloud cryptography), the client needs a way to verify the authenticity of the device protecting their most valued cryptographic keys.

Public Key Confirmations

Thales Group's SafeNet Luna HSMs include factory-issued device identities certified by a Thales Group authority. The root of this authority is maintained by Thales Group in HSMs locked in a vault with layered physical and logical access controls. These certificates are used as the root of trust for the issuance of "public key confirmations" (PKCs), certificates issued by the HSM attesting to the life cycle of a specific private key. A Luna HSM will issue confirmations only for private keys that were created by the HSM and that can never exist outside of the HSM. A valid confirmation is cryptographic proof that a specific key is inside the identified HSM. The confirmation is also proof that that the identified HSM is real.

The key pair within the HSM that signs the confirmation is called a Hardware Origin Key (HOK). It is protected inside the HSM's FIPS 140-2 Level 3 security boundary. Each HOK is unique and there is no way to extract or replace it. The HOK is created in the HSM at the time of manufacture and certified by Thales Group's secure manufacturing authority, which is certified by Thales Group's root authority.

Public key confirmations are automatically generated for RSA key pairs in the HSM. A user can get a confirmation through the PKCS #11 API or the Luna **cmu** tool, and use it to verify that any RSA key is protected and has always been protected by a Luna HSM. A PKC bundle contains the following certificates:

- **MIC:** Manufacturing Integrity Certificate; corresponds to the Manufacturing Integrity Private Key (MIK), signed by the SafeNet Root.
- **HOC:** Hardware Origin Certificate; corresponds to the Hardware Origin Private Key (HOK). Unique to each HSM. Signed by MIK.
- **DAC:** Device Authentication Certificate; corresponds to the Device Authentication Private Key (DAK). Unique to each HSM. Signed by HOK.
- **PKC:** Public Key Confirmation Certificate; certificate for a private key on the HSM. Signed by DAK.

Public key confirmations are delivered as PKCS #7 files containing a certificate chain. The PKCS #7 files can be viewed using tools like OpenSSL and Microsoft's Certificates snap-in for MMC.

> **NOTE** While third-party tools are capable of cryptographically validating the certificate signature chain, they may display some certificate errors, since they do not recognize some SafeNet-specific key usage attributes included in the certificates.

Chains of Trust

The chain of trust available via the **cmu** utility included with the SafeNet Luna HSM Client, **Chrysalis-ITS**, is built in by default, and originates from Thales's root certificate authority. It uses the MIC, HOC, DAC, and the PKC.

> **NOTE** Since the introduction of Functionality Modules, HSMs are shipped from the factory with FM-ready hardware. This means that they contain, and use, the HOK and the HOC, but they also have the FM-HOK and FM-HOC on standby. If FMs are enabled on the HSM, the original HOK and HOC are deleted, and the chain-of-trust, thereafter, proceeds through the FM-HOC.

Confirming the HSM's Authenticity

The **cmu** utility also includes a command that tests an HSM's authenticity by creating and verifying a confirmation on a temporary key created in the HSM (see "cmu verifyhsm" on page 1 in the *Utilities Guide*). The test includes a proof of possession that asks the HSM to sign a user-entered string as proof the associated private key is present within the target HSM.

> **NOTE** This confirmation procedure is currently not supported on FM-enabled HSMs. Refer to "FM Deployment Constraints" on page 1 for details.

The test requires the SafeNet root certificate, provided below:

safenet-root.pem

> **NOTE** The current certificate is valid until 2031-12-31, but it might change before this date at Thales Group's discretion. Ensure that you have the most recent version of this documentation.

To confirm the HSM's authenticity

1. Right-click the link above and save the root certificate to the SafeNet Luna HSM Client directory.
2. Open a command line and navigate to the SafeNet Luna HSM Client directory.
3. Use the **cmu** utility to authenticate the HSM. You must specify a challenge string for the HSM to sign, and the root certificate file:

   >**cmu verifyhsm -challenge** <string> **-rootcert safenet-root.pem**

   When prompted, specify the partition you wish to use and the Crypto Officer credential for that partition.

```
>cmu verifyhsm -challenge "1234567890" -rootcert safenet-root.pem
Select token
 [0] Token Label: mypartition-1
 [1] Token Label: mypartition-2
 Enter choice: 0
Please enter password for token in slot 0 : ********
Reading rootcert from file "safenet-root.pem"... ok.
Generating temporary RSA keypair in HSM... ok.
Extracting PKC bundle from HSM... ok.
Verifying PKC certificate... ok.
Verifying DAC certificate... ok.
Verifying HOC certificate... ok.
Verifying MIC certificate... ok.
Verifying MIC against rootcert... ok.
Signing and verifying challenge... ok.
Verifying HSM serial number... ok.
Overall status: Success.
```

If this test fails, contact the HSM SO.