# SafeNet PCIe HSM

Configuration Guide

security to be free

## Document Information

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

## Revision History

| Revision | Date | Reason |
|---|---|---|
| A | 26 July 2016 | Initial release. |

## Trademarks

## Acknowledgements

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

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

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

This product uses Brian Gladman’s AES implementation.

Refer to the End User License Agreement for more information.

## 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 SafeNet-supplied or approved accessories.

### USA, FCC

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

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

**Note:** This equipment has been tested and found to comply with the limits for a “Class B” digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

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

### Canada

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

### Europe

This product is in conformity with the protection requirements of EC Council Directive 2004/108/EC. Conformity is declared to the following applicable standards for electro-magnetic compatibility immunity and susceptibility; CISPR22and IEC801. This product satisfies the CLASS B limits of EN 55022.

## Disclaimer

Gemalto makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Gemalto reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Gemalto to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Gemalto invites constructive comments on the contents of this document. Send your comments, together with your personal and/or company details to the address below.

| Contact Method | Contact Information |
|---|---|
| Mail | Gemalto<br>4690 Millennium Drive<br>Belcamp, Maryland 21017<br>USA |
| Email | techpubs@safenet-inc.com |

# CONTENTS

# PREFACE

# About the Configuration Guide

This document describes how to configure your HSM to get it ready to operate in your environment. Configuring an HSM consists of:

- Initializing the HSM - establishing ownership on the part of a role called the HSM Security Officer (SO) "Initialize the HSM " on page 12
  - Initializing a Password-authenticated HSM "Initializing a Password Authenticated HSM" on page 14
  - Initializing a PED-authenticated HSM "Initializing a SafeNet PED-Authenticated PCIe HSM" on page 16
- Setting HSM Policies - configuration settings to adjust some security and behavior parameters
- Creating a working space on the HSM for your application programs, called an application partition, in either of two types
  - Creating a legacy-style application partition (owned/managed by the same SO that owns the HSM)<br>
    -- Creating a legacy partition on a Password-authenticated HSM<br>
    -- Creating a legacy partition on a PED-authenticated HSM
  - Creating a Per-Partition SO application partition (which has its own SO and is independent of the HSM SO)<br>
    -- Creating a PPSO partition on a Password-authenticated HSM<br>
    -- Creating a PPSO partition on a PED-authenticated HSM
- "Optional Configuration Tasks" on page 1

This preface also includes the following information about this document:

- "Customer Release Notes" below
- "Gemalto Rebranding" on the next page
- "Audience" on the next page
- "Document Conventions" on the next page
- "Support Contacts" on page 9

For information regarding the document status and revision history, see "Document Information" on page 2.

## Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN for this release at the following location:

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

# Gemalto Rebranding

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

| Old product name | New product name |
|---|---|
| Luna SA HSM | SafeNet Network HSM |
| Luna PCI-E HSM | SafeNet PCIe HSM |
| Luna G5 HSM | SafeNet USB HSM |
| Luna PED | SafeNet PED |
| Luna Client | SafeNet HSM Client |
| Luna Dock | SafeNet Dock |
| Luna Backup HSM | SafeNet Backup HSM |
| Luna CSP | SafeNet CSP |
| Luna JSP | SafeNet JSP |
| Luna KSP | SafeNet KSP |

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

# Audience

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

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

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

# Document Conventions

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

## Notes

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

**Note:** Take note. Contains important or helpful information.

## Cautions

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

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

## Warnings

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

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

## Command syntax and typeface conventions

| Format | Convention |
|---|---|
| **bold** | The bold attribute is used to indicate the following:<br>• Command-line commands and options (Type dir /p.)<br>• Button names (Click Save As.)<br>• Check box and radio button names (Select the Print Duplex check box.)<br>• Dialog box titles (On the Protect Document dialog box, click Yes.)<br>• Field names (User Name: Enter the name of the user.)<br>• Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.)<br>• 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. Omit the brackets when typing the command. |
| [**optional**]<br>[<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. Omit the square or angle brackets when typing the command. |
| {**a**\|**b**\|**c**}<br>{<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. |

| Format | Convention |
|---|---|
| [**a**\|**b**\|**c**]<br>[<a>\|<b>\|<c>] | Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars. |

## Support Contacts

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

| Contact method | Contact |
|---|---|
| | to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base. |

# Introduction

After your SafeNet HSM has been unpacked and installed, and the associated SafeNet HSM Client software is installed on the host computer, a few configuration steps remain, to prepare the HSM for use with your client application (s). Some 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, assigning a Security Officer role, to oversee and administer the HSM. Then you can apply some optional, global settings.

- "Configuring a Password-Authenticated HSM" on page 13

  or

- "Configuring a PED-Authenticated HSM" on page 15

  and optionally

- "Set the HSM Policies" on page 23.

The second task declares a special area within the HSM called an application partition, that your application accesses, to create, store, and use keys, certificates, and other crypto objects. Part of the task is to choose a style of interaction,

- either one that we have termed "legacy", where the HSM SO retains ownership and oversight of the application partition, and the HSM SO creates a Crypto Officer to handle access-control by applications,
- or the newer Per-Partition Security Officer (PPSO) style, where a Partition SO is created to oversee the application partition, and the HSM SO has no further interaction, and no ability to see, inside the partition; the Partition SO sets policies and performs other administration within the application partition, and creates a Crypto Officer to handle access-control by applications.

The HSM must be initialized (above) before the HSM SO can create an application partition of any style. See

"Create a Legacy Password-authenticated Application Partition " on page 41 or "Overview - Configure a PED-Authenticated Application Partition" on page 56

# 3
# Initialize the HSM

In this chapter you will initialize your HSM. To initialize an HSM is to prepare it for operation under the control of an HSM Security Officer or SO (the entity that administers the HSM).

## Password-Authenticated versus PED-Authenticated HSMs

The HSM is available in PED-authenticated or password-authenticated versions. Follow the initialization steps in this chapter to initialize the type of HSM that you have purchased.

There is no externally visible difference between a password-authenticated or PED-authenticated HSM. For an installed HSM, you can determine its mode of authentication by attempting to log in. A PED-authenticated version will direct you to the SafeNet PED. A Password Authenticated version will prompt you for the password. You cannot change the authentication type of a SafeNet HSM. It is a manufacturing configuration, set at the factory. If you have a PED-authenticated version, you cannot access the HSM and partitions by means of passwords.

For password-authenticated HSMs, you authenticate to the HSM as Security Officer, or Crypto Officer, or User, etc., by typing a password on your computer keyboard.

For PED-authenticated HSMs, you authenticate to the HSM as Security Officer, or Crypto Officer, or User, etc., by presenting an iKey PED Key device that contains the authentication.

### Which kind do I have?

SafeNet HSMs are shipped from the factory as one or the other type. This is not a field-changeable setting. If you are not sure which kind you have, verify the type of HSM with the command

**hsm showinfo** in lunacm.

That command is one of several non-sensitive HSM commands that does not require HSM authentication. The output lists the configuration packages (additions to the basic build) that make up your SafeNet HSM. Look for the term **FIPS3** appearing in that list to indicate that your SafeNet HSM is PED Authenticated - otherwise, your HSM is Password Authenticated.

See a comparison of Password-authenticated versus PED-authenticated at "Comparing Password and PED Authentication" on page 1.

### What if I make a mistake about the type of authentication I present?

No harm. Offering the wrong kind of authentication is not harmful - the only result is a brief delay. However, offering the wrong authentication of the correct type starts the counter for "bad login" attempts. The following paragraphs offer a little more detail.

As a general rule, when you attempt to login to the HSM or to issue any command that requires authentication, the command-line prompts you for the needed authentication. If yours is a Password Authenticated HSM, you are asked for the password, and the command eventually times out if the password is not given. (Of course, if you provide a wrong password, that is applied against the count of bad login attempts. However, connecting a PED and offering a PED Key to a Password Authenticated HSM has no effect; it is ignored.)

If yours is a PED Authenticated (Trusted Path) HSM, the prompt asks you to attend to the PED for further instructions. If a PED is not connected and/or you don't supply the appropriate PED Keys and keypad actions, the command eventually times out. (If you do have a PED connected and supply the wrong PED Key [of the type requested], then that action is applied against the count of bad login attempts. However, if you mistakenly provide a password [at the command-line] for a PED Authenticated SafeNet HSM, that password is ignored and the bad-login-attempt count is not incremented.)

In either case, just wait for the timeout (a few minutes) to conclude, then begin again, using the correct authentication method.

> **Note:** We recommend that you read through the pages in the Configuration Guide at least once in advance of starting the procedure, so that you can resolve any questions before beginning any time-limited operations. For a Password Authenticated SafeNet HSM, you should have passwords already determined according to your organization's security policies. For a PED Authenticated SafeNet HSM, you should have a SafeNet PED connected, and an appropriate set of PED Keys available.

If this is your only PED Authenticated SafeNet HSM, then you should have received a PED and PED Keys along with the HSM/appliance. If you have other PED Authenticated units at your location, then you can use a PED from one of them.

## High-Level Configuration Steps

1. Initialize the HSM. Choose one or the other of:
   a. "Initializing a SafeNet PED-Authenticated PCIe HSM" on page 16
   b. "Initializing a Password Authenticated HSM" on the next page.
2. Change the HSM policies, if desired, as described in

   "Setting SafeNet PCIe HSM Policies, PED-authenticated [Optional]" on page 30.

   If any of the policies you set are destructive, you must re-initialize the HSM after setting the polices.
3. Create a partition on the HSM, as described in

   "Creating a Legacy-style PED-authenticated Application Partition" on page 56.
4. Change the partition policies, if desired, as described in "Setting SafeNet PCIe HSM Partition Policies [Optional] " on page 73

# Configuring a Password-Authenticated HSM

This section describes how to configure a password-authenticated HSM to get it ready to operate in your environment. It contains the following sections:

- "About Initializing a Password-Authenticated HSM" on the next page
- "Setting SafeNet PCIe HSM Policies, PW-authenticated [Optional]" on page 23

After that, go on to creating an application partition

# About Initializing a Password-Authenticated HSM

In this section, you initialize the HSM, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your SafeNet HSM.

Initialization prepares the HSM for use by setting up the necessary identities, ownership and authentication that are to be associated with the HSM. You must initialize an HSM one time before you can generate or store objects, allow clients to connect, or perform cryptographic operations.

Once you have initialized an HSM, you would return to this section only to clear an entire HSM and all its contents and HSM Partitions, by re-initializing.

Go to "Initializing a Password Authenticated HSM" below.

## Initializing a Password Authenticated HSM

Initialize the HSM to set up the necessary identities, ownership and authentication on the HSM. This is required before you can create Partitions and use the HSM.

### Start the Initialization Process

The `hsm init` command takes several options.

See "hsm init" on page 1 in the *Lunacm Command Reference*.

For an HSM with Password Authentication, you need to provide a label, password, and cloning domain. The only one that you should type at the command line is the label. The password and cloning domain can be typed at the command line, but this makes them visible to anyone who can see the computer screen, or to anyone who later scrolls back in your console or ssh session buffer.

If you omit the password and the domain, the system prompts you for them, and hides your input with "*" characters. This is preferable from a security standpoint. Additionally, you are prompted to re-enter each string, thus helping to ensure that the string you type is the one you intended to type.

#### Label

The label is a string of up to 32 characters that identifies this HSM unit uniquely. A labeling convention that conveys some information relating to business, departmental or network function of the individual HSM is commonly used.

#### HSM password

The HSM password is a password for the HSM Security Officer (SO).

It should employ standard password-security characteristics:

- at least 8 characters,
- not easily guessable (therefore, no words that occur in any dictionary)
- no dates like birthdays or anniversaries, no proper names
- should include miXEd-CAse letters, numbers, special (non-alphanumeric, -_!@#$%&*...).

#### Cloning domain

The cloning domain is a shared identifier that makes cloning possible among a group of HSMs. Cloning is required for backup or for HA. Cloning cannot take place between HSMs that do not share a common domain.

Always specify a cloning domain when you initialize a Password Authenticated SafeNet 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 the time being, for benefit of customers who have previously used the default domain. When you prepare a SafeNet HSM to go into service in a real "production" environment, always specify a proper, secure domain string when you initialize.

### Initialize a Password Authenticated HSM

Type the `hsm init` command at the prompt, supplying a text label for the new HSM.

```
lunacm:> hsm init -label myluna1

Option -password was not supplied.  It is required.
Enter the password: *********
Re-enter the password: *********

Option -domain not specified.
If you proceed, the default domain will be used.
You will not be creating a new domain.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Command Result : No Error
lunacm:>
```

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

You have initialized the HSM and created an HSM SO identity to perform global administrator activities on the HSM, including creating other identities for special roles and purposes.

You are ready to adjust HSM Policies (if desired) and begin creating HSM Partitions for your Client's applications to use.

Go to "Set HSM Policies (Password Authentication)"

# Configuring a PED-Authenticated HSM

This section describes how to configure a PED-authenticated HSM to get it ready to operate in your environment. It contains the following sections:

- " About Initializing a PED-Authenticated HSM" on the next page
- "Setting SafeNet PCIe HSM Policies, PED-authenticated [Optional]" on page 30

After that, go on to creating an application partition

# About Initializing a PED-Authenticated HSM

In this section, you initialize the HSM, and set any policies that you require. In normal operation, you would perform these actions just once, when first commissioning your SafeNet HSM.

Initialization prepares the HSM for use by setting up the necessary identities, ownership and authentication that are to be associated with the HSM. You must initialize an HSM one time before you can generate or store objects, allow clients to connect, or perform cryptographic operations.

If you have not used SafeNet HSMs and PED Keys before, please read the sub-section ""PED Key Management Overview" on page 1" in the *Administration Guide*, before you start initializing.

Once you have initialized an HSM, you would return to this section only to clear an entire HSM and all its contents and HSM Partitions, by re-initializing.

If you received your SafeNet HSM in Secure Transport Mode, then a preliminary step is required before you can initialize; see "Recover the SRK".

Otherwise, go directly to "Initializing a SafeNet PED-Authenticated PCIe HSM" below.

# Initializing a SafeNet PED-Authenticated PCIe HSM

Your SafeNet PCIe HSM 5 HSM arrives in "Zeroized" state, and in a default, pre-initialized condition (see below). It might also be in Secure Transport Mode, if you selected that option at purchase time.

### To determine the state of the HSM

The LunaCM utility presents status information for connected HSMs when lunacm is launched.

```
bash-3.00# ./lunacm
LunaCM V2.3.3 - Copyright (c) 2006-2010 SafeNet, Inc.
Available HSMs:
Slot Id ->               1
Tunnel Slot Id ->        3
HSM Label ->             no label
HSM Serial Number ->     151433
HSM Model ->             K6 Base
HSM Firmware Version -> 6.2.1
HSM Configuration ->     Luna PCI (PED) Undefined Mode / Uninitialized
HSM Status ->            Transport Mode, Zeroized
Slot Id ->               2
Tunnel Slot Id ->        4
HSM Label ->             no label
HSM Serial Number ->     151446
HSM Model ->             K6 Base
HSM Firmware Version -> 6.2.1
HSM Configuration ->     Luna PCI (PED) Undefined Mode / Uninitialized
HSM Status ->            Transport Mode, Zeroized
Current Slot Id: 1
lunacm:>
```

“Transport Mode” refers to a user-invoked tamper event.

“Zeroized” state results from the battery being disengaged and the Real Time Clock and the battery-backed memory left un-powered. This renders any HSM contents unrecoverable (at the factory, we would have created only unimportant test objects on the HSM - if you have previously had the HSM in service, and then either "decommissioned" it or performed `hsm factoryreset` your valid objects and keys are similarly rendered permanently unrecoverable and the HSM is completely safe to store or ship ).

The above two states are addressed by configuring and initializing your SafeNet PCIe HSM 5 HSM. Instructions start on this page.

If you requested Secure Transport Mode shipment from SafeNet, then a couple of additional steps are required (also included in these instructions).

## Why Initialize?

Before you can make use of it, the HSM must be initialized. This establishes your ownership for current and future HSM administration. Initialization assigns a meaningful label, as well as Security Officer authentication (PED Key) and Domain (another PED Key), and places the HSM in a state ready to use.

Use the instructions on this page if you have SafeNet PCIe HSM with PED (Trusted Path) authentication.

Some HSM Policy changes are destructive. A destructive policy change is one that requires the HSM to be initialized again, before it can be used. Thus if you intend to perform a destructive HSM Policy change, you might need to perform this initialization step again, after the Policy change.

### Start the lunacm Utility

```
C:\Program Files\LunaPCI>lunacm
LunaCM V2.3 - Copyright (c) 2006-2010 SafeNet, Inc.
Available HSMs:
Slot Id ->                1
Tunnel Slot Id ->         2
HSM Label ->              no label
HSM Serial Number ->      8000001
HSM Model ->              K6Base
HSM Firmware Version -> 6.1.3
HSM Configuration ->      Luna PCI (PED) Signing with Cloning Mode
Current Slot Id: 1
lunacm:>
```

Notice that the HSM does not yet have a label, indicating that it has not been initialized since manufacture.

### Initialize the HSM

1. Have the SafeNet PED connected and ready (in local mode and "Awaiting command...").
2. Insert a blank PED Key into the USB connector at the top of the PED.
3. In a terminal window (DOS command-line window in Windows), go to the LunaPCI directory and start the lunacm utility:
   lunacm:>
4. Run the "hsm init" command, giving a label for your SafeNet PCIe HSM. If Secure Transport Mode was set, you must unlock the HSM with the purple PED Key before you can proceed.

   The following is an example of initialization dialog, with PED interactions inserted to show the sequence of events.

   ```
   lunacm:> hsm init -label myPCI
   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
   Please attend to the PED.
   ```

5. SafeNet PED asks preliminary setup questions [ The simplest scenario is your first-ever HSM and new PED Keys. However, you might have previously initialized this HSM and be starting over. Or you might have other HSMs already initialized and need to share the authentication or the domain with your new HSM. ] the HSM and PED need to know, prior to imprinting the first HSM Adminstrator / SO PED Key.

   ```
   Slot 01
   SETTING SO PIN...
   Would you like to
   reuse an existing
   keyset? (Y/N)
   ```

6. If you say [ NO ] (on the PED keypad), then you are indicating there is nothing of value on your PED Keys to preserve. On the assumption that you will now be writing onto a new blank PED Key, or onto one that contains old unwanted authentication, SafeNet PED asks you to set MofN values.

   ```
   Slot 01
   SETTING SO PIN...
   M value? (1-16)
   >01
   ```

   and

   ```
   Slot 01
   SETTING SO PIN...
   N value? (M-16)
   >01
   ```

   Setting M and N equal to "1" means that the authentication is not to be split, and only a single PED Key will be necessary when the authentication is called for in future.

   Setting M and N larger than "1" means that the authentication is split into N different "splits", of which quantity M of them 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 other holders.

7. 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.

   SafeNet PED now asks you to provide the appropriate PED Key - a fresh blank key, or a previously used key that you intend to overwrite, or a previously used key that you intend to preserve and share with this HSM.

   ```
   SLOT 01
   SETTING SO PIN...
   Insert a SO /
   HSM Admin
   PED Key.
   Press ENTER.

   Slot 01
   SETTING SO PIN...
   **WARNING**
   This PED Key is
   blank.
   Overwrite?   YES/NO
   ```

   OR

   ```
   Slot 01
   Initialize HSM
   **WARNING**
   ```

```
This PED Key is for
SO / HSM Admin.
Overwrite?   YES/NO
```

8. Answer (press the appropriate button on the PED keypad)

   - "**NO**" if the PED key that you provided carries SO authentication data that must be preserved. In that case, you must have made a mistake so the PED goes back to asking you to insert a suitable key.
   - "**YES**" if the PED should overwrite (if you overwrite a never-used PED Key, nothing is lost; 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 - therefore "YES" means 'yes, destroy the contents on the key and create new authentication information in its place' - be sure that this is what you wish to do) the PED Key with a new SO authentication. (This will be matched on the SafeNet PCIe HSM during this initialization).

9. SafeNet PED makes very sure that you wish to overwrite, by asking again.

   ```
   SLOT 01
   SETTING SO PIN...
   ***WARNING **
   Are you sure you
   want to overwrite
   this PED Key? YES/NO
   ```

10. For any situation other than reusing a keyset, SafeNet PED now prompts for you to set a PED PIN. For multi-factor authentication security, the 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 01
    SETTING SO PIN...
    Enter new PED PIN:

    Confirm new PED PIN:
    ```

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

    SafeNet PED imprints the PED Key, or the HSM, or both, as appropriate, and then prompts the final question for this key:

    ```
    SLOT 01
    SETTING SO PIN...
    Are you duplicating
    this keyset? (Y/N)
    ```

12. You can respond [ YES ] and present one or more blank keys, all of which will be imprinted with exact copies of the current PED Key's authentication, or you can say [ NO ], telling the PED to move on to the next part of the initialization sequence. (You should always have backups of your imprinted PED Keys, to guard against loss or damage.)

13. To begin imprinting a Cloning Domain (red PED Key), you must first log into the HSM, so you can simply leave the blue PED Key in place.

    ```
    SLOT 01
    SO LOGIN...
    Insert a SO /
    HSM Admin
    ```

```
PED Key.
Press ENTER.
```

14. SafeNet PED passes the authentication along to the HSM and then asks the first question toward imprinting a cloning domain:

```
SLOT 01
SO SETTING DOMAIN...
Would you like to
reuse an existing
keyset? (Y/N)
```

If this is your first SafeNet HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized, then answer [ NO ]. SafeNet PED prompts for values of M and N.

If you have another HSM and wish that HSM and the current HSM to share their cloning Domain, then you must answer [ YES ]. In that case, SafeNet PED does not prompt for M and N.

```
SLOT 01
SO SETTING DOMAIN...
M value? (1-16)

>01
SLOT 01
SO SETTING DOMAIN...
M value? (1-16)

>01
```

SafeNet PED goes through the same sequence that occurred for the blue SO PED Key, except it is now dealing with a red Domain PED Key.

```
SLOT 01
SO SETTING DOMAIN...
Insert a
Domain
PED Key
Press ENTER.

Slot 01
SO SETTING DOMAIN...
**WARNING**
This PED Key is
blank.
Overwrite?   YES/NO
```

OR

```
Slot 01
SO SETTING DOMAIN...
**WARNING**
This PED Key is for
Domain.
Overwrite?   YES/NO
```

Just as with the blue SO PED Key, the next message is:

```
Slot 01
SO SETTING DOMAIN...
**WARNING**
Are you sure you
```

```
want to overwrite
this PED Key?   YES/NO
```

15. When you confirm that you do wish to overwrite whatever is (or is not) on the currently inserted key, with a Cloning Domain generated by the PED, the PED asks:

```
Slot 01
SO SETTING DOMAIN...
Enter new PED PIN:

Confirm new PED PIN:
```

    And finally:

```
SLOT 01
SO SETTING DOMAIN...
Are you duplicating
this keyset? (Y/N)
```

16. Once you stop duplicating the Domain key, or you indicate that you do not wish to make any duplicates (you should have backups of all your imprinted PED Keys...), SafeNet PED goes back to "Awaiting command...".

    Lunacm says:

```
Command Result : No Error
lunacm:>
lunacm:> hsm showinfo
       HSM
 Label -> myLuna
       HSM Manufacturer -> Safenet, Inc.
       HSM Model -> K6 Base
       HSM Serial Number -> 150022
       HSM Status -> OK
       Token Flags ->
            CKF_RNG
            CKF_LOGIN_REQUIRED
            CKF_USER_PIN_INITIALIZED
            CKF_RESTORE_KEY_NOT_NEEDED
            CKF_TOKEN_INITIALIZED
       Firmware Version -> 6.2.1
       Rollback Firmware Version -> Not Available
       Slot Id -> 1
       Tunnel Slot Id -> 2
       Session State -> CKS_RW_PUBLIC_SESSION
       SO Status->        Not Logged In
       SO Failed Logins-> 0
       SO Flags ->
            CONTAINER_KCV_CREATED
       HSM Storage:
            Total Storage Space:  2097152
            Used Storage Space:   2097152
            Free Storage Space:   0
            Allowed Partitions:   1
            Number of Partitions: 1
       SO Storage:
            Total Storage Space:  262144
            Used Storage Space:   0
            Free Storage Space:   262144
            Object Count:         0
```

```
*** The HSM is NOT in FIPS 140-2 approved operation mode. ***
License Count -> 7
            1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
            2. 620127-000 ECC
            3. 620114-001 Cloning
            4. 620109-000 FIPS3
            5. 621010358-001 621-010358-001 External MTK - STM disabled
            6. 621010089-001 621-010089-001 Remote Ped
            7. 621000021-001 SCU K5/K6 Performance 15
Command Result : No Error
lunacm:>
```

Notice that the HSM now has a label. If you were to exit and restart the lunacm utility, you would see the new label that you have just applied to the HSM.

17. The next step is to create a partition on the HSM. See "Creating a Legacy-style PED-authenticated Application Partition" on page 56.

# 3
# Set the HSM Policies

SafeNet HSMs are built on one of our general-purpose HSM platforms (hardware plus firmware), and then are loaded with what we call "personality", to make them into specific types of HSM with specific abilities and constraints, to suit different markets and applications.

The built-in attributes are called "Capabilities" and describe what the HSM can do as it comes to you from the factory.

Some capabilities are unalterable, except by re-manufacturing the HSM.

Many HSM capabilities can be altered by means of HSM Policies, which coincide one-for-one with the capabilities that they alter.

You can view the current HSM capabilities and policies with the **hsm showpolicies** command:

You can change a current HSM policy in lunacm with the **hsm changeHMSPolicy** 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 PCIe HSM Policies, PW-authenticated [Optional]" below
- "Setting SafeNet PCIe HSM Policies, PED-authenticated [Optional]" on page 30

## Setting SafeNet PCIe HSM Policies, PW-authenticated [Optional]

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 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.

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

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0

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


        License Count -> 7
                1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                2. 620127-000 ECC
                3. 620114-001 Cloning
                4. 620127-000 Test K3 ECC Update - 620127
                5. 621010358-001 621-010358-001 External MTK - STM disabled
                6. 621010089-001 621-010089-001 Remote Ped
                7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
lunacm:>
```

Note the message near the end, 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 : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 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
                20: Enable Remote Authentication : 1
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 1
                26: Enable External Storage of MTK Split : 1
                27: HSM non-volatile storage space : 2097152
                28: Enable HA mode CGX : 0
                29: Enable Acceleration : 1
                30: Enable unmasking : 1

        HSM Policies
                0: PIN-based authentication : 0
                1: PED-based authentication : 1
                6: Allow masking : 1
                7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 1
                15: SO can reset partition PIN : 1
                16: Allow network replication : 1
                20: Allow Remote Authentication : 1
                21: Force user PIN change after set/reset : 0
                22: Allow offboard storage : 1
                23: Allow partition groups : 0
                25: Allow remote PED usage : 1
                26: Store MTK Split Externally : 1
                29: Allow Acceleration : 1
                30: Allow unmasking : 1

        SO 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
                14: Enable PED use without challenge : 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 : 3
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        SO 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
                14: Challenge for authentication not needed : 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 : 3
                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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

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 SafeNet PED (SafeNet PED must be connected and ready before you login). For a password-authenticated HSM the password is needed, and no PED is involved), then type the `hsm changeHSMPolicy` or the `hsm changeSOPolicy` command:

```
lunacm:> hsm login
Please attend to the PED
```

> **Note:** At this time, you must respond to the prompts on the SafeNet PED screen.

```
command Result : No error
lunacm:>
hsm changeHSMPolicy -policy 12 -value 0
command Result : No error

lunacm:>
```

```
lunacm:> hsm showpolicies

        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                2: Performance level : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 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
                20: Enable Remote Authentication : 1
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 1
                26: Enable External Storage of MTK Split : 1
                27: HSM non-volatile storage space : 2097152
                28: Enable HA mode CGX : 0
                29: Enable Acceleration : 1
                30: Enable unmasking : 1

        HSM Policies
                0: PIN-based authentication : 0
                1: PED-based authentication : 1
                6: Allow masking : 1
                7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 0
                15: SO can reset partition PIN : 1
                16: Allow network replication : 1
                20: Allow Remote Authentication : 1
                21: Force user PIN change after set/reset : 0
                22: Allow offboard storage : 1
                23: Allow partition groups : 0
                25: Allow remote PED usage : 1
                26: Store MTK Split Externally : 1
                29: Allow Acceleration : 1
                30: Allow unmasking : 1

        SO 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
                14: Enable PED use without challenge : 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 : 3
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        SO 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
                14: Challenge for authentication not needed : 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 : 3
                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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
lunacm:> hsm showinfo

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
```

```
                    CKF_RESTORE_KEY_NOT_NEEDED
                    CKF_PROTECTED_AUTHENTICATION_PATH
            Firmware Version -> 6.1.3
            Rollback Firmware Version -> 6.1.0
            Slot Id -> 1
            Tunnel Slot Id -> 2
            Session State -> CKS_RW_PUBLIC_SESSION

            SO Status->        Not Logged In
            SO information is not available (HSM has not been initialized)

            HSM Storage:
                    Total Storage Space:  2097152
                    Used Storage Space:   0
                    Free Storage Space:   2097152
                    Allowed Partitions:   20
                    Number of Partitions: 0

            SO Storage:
                    Total Storage Space:  262144
                    Used Storage Space:   0
                    Free Storage Space:   262144
                    Object Count:         0

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


            License Count -> 7
                    1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                    2. 620127-000 ECC
                    3. 620114-001 Cloning
                    4. 620127-000 Test K3 ECC Update - 620127
                    5. 621010358-001 621-010358-001 External MTK - STM disabled
                    6. 621010089-001 621-010089-001 Remote Ped
                    7. 621000021-001 SCU K5/K6 Performance 15

    Command Result : No Error
    lunacm:>
```

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 algorithms : **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.

### Second Example – Destructive Change of HSM Policy

```
lunacm:> hsm -changeHSMPolicy -policy 15 -value 0
```

That command assigns a value of zero (0) to the “Enable SO reset of partition PIN” policy, turning it off.

The above example is a change to a destructive policy, meaning 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 HSM has been in a “live” or “production” environment and contains useful or important data, keys, certificates.

The work-around is to 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.

# Setting SafeNet PCIe HSM Policies, PED-authenticated [Optional]

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 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.

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

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:    0
                Free Storage Space:    262144
                Object Count:          0

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


        License Count -> 7
                1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                2. 620127-000 ECC
                3. 620114-001 Cloning
                4. 620127-000 Test K3 ECC Update - 620127
                5. 621010358-001 621-010358-001 External MTK - STM disabled
                6. 621010089-001 621-010089-001 Remote Ped
                7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
lunacm:>
```

Note the message near the end, 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 : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 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
                20: Enable Remote Authentication : 1
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 1
                26: Enable External Storage of MTK Split : 1
                27: HSM non-volatile storage space : 2097152
                28: Enable HA mode CGX : 0
                29: Enable Acceleration : 1
                30: Enable unmasking : 1

        HSM Policies
                0: PIN-based authentication : 0
                1: PED-based authentication : 1
                6: Allow masking : 1
                7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 1
                15: SO can reset partition PIN : 1
                16: Allow network replication : 1
                20: Allow Remote Authentication : 1
                21: Force user PIN change after set/reset : 0
                22: Allow offboard storage : 1
                23: Allow partition groups : 0
                25: Allow remote PED usage : 1
                26: Store MTK Split Externally : 1
                29: Allow Acceleration : 1
                30: Allow unmasking : 1

        SO 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
                14: Enable PED use without challenge : 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 : 3
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        SO 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
                14: Challenge for authentication not needed : 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 : 3
                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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

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 SafeNet PED (SafeNet PED must be connected and ready before you login). For a password-authenticated HSM the password is needed, and no PED is involved), then type the `hsm changeHSMPolicy` or the `hsm changeSOPolicy` command:

```
lunacm:> hsm login
Please attend to the PED
```

**Note:** At this time, you must respond to the prompts on the SafeNet PED screen.

```
command Result : No error
lunacm:>
hsm changeHSMPolicy -policy 12 -value 0
command Result : No error

lunacm:>
lunacm:> hsm showpolicies

        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                2: Performance level : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 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
                20: Enable Remote Authentication : 1
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 1
                26: Enable External Storage of MTK Split : 1
                27: HSM non-volatile storage space : 2097152
                28: Enable HA mode CGX : 0
                29: Enable Acceleration : 1
                30: Enable unmasking : 1

        HSM Policies
                0: PIN-based authentication : 0
                1: PED-based authentication : 1
                6: Allow masking : 1
                7: Allow cloning : 1
                12: Allow non-FIPS algorithms : 0
                15: SO can reset partition PIN : 1
                16: Allow network replication : 1
                20: Allow Remote Authentication : 1
                21: Force user PIN change after set/reset : 0
                22: Allow offboard storage : 1
                23: Allow partition groups : 0
                25: Allow remote PED usage : 1
                26: Store MTK Split Externally : 1
                29: Allow Acceleration : 1
                30: Allow unmasking : 1

        SO 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
                14: Enable PED use without challenge : 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 : 3
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        SO 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
                14: Challenge for authentication not needed : 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 : 3
                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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
lunacm:> hsm showinfo

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0
```

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


            License Count -> 7
                    1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                    2. 620127-000 ECC
                    3. 620114-001 Cloning
                    4. 620127-000 Test K3 ECC Update - 620127
                    5. 621010358-001 621-010358-001 External MTK - STM disabled
                    6. 621010089-001 621-010089-001 Remote Ped
                    7. 621000021-001 SCU K5/K6 Performance 15

    Command Result : No Error
    lunacm:>
```

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 algorithms : **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.

### Second Example – Destructive Change of HSM Policy

```
lunacm:> hsm -changeHSMPolicy -policy 15 -value 0
```

That command assigns a value of zero (0) to the “Enable SO reset of partition PIN” policy, turning it off.

The above example is a change to a destructive policy, meaning 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 HSM has been in a “live” or “production” environment and contains useful or important data, keys, certificates.

The work-around is to 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.

# 3 Creating an Application Partition in the HSM

In a previous chapter, you initialized the HSM, establishing ownership and administrative oversight by an entity called 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.

Two variables come into play, to determine which set of instructions should apply to your HSM and application partition:

- the type of authentication used by your HSM, and therefore by any application partitions (which was decided when you purchased the HSM), and
- the style of partition that you are about to create (discussed in the next section).

## Choose Partition Type

The options are:

- Legacy-style application partitions are owned and administered by the HSM SO, who retains complete control.
- PPSO-style application partitions each have their own SO, independent of the HSM SO, and all administrative control, except partition deletion, resides with the Partition SO

### Legacy-style Partitions

Choose the authentication method that applies to your HSM.

See "Create a Legacy Password-authenticated Application Partition " on page 41 .

See "Create a PED Authenticated Legacy-style Application Partition (f/w pre-6.22.0)" on page 1.

### Per-Partition SO (PPSO) Partitions

For an overview of the procedure to set up a PPSO partition, see "About Configuring an Application Partition with Its Own SO " on the next page.

# About Configuring an Application Partition with Its Own SO

When you are ready to create and configure an application partition, it is assumed that you have already initialized and configured the HSM that is to contain the application partition.

SafeNet HSMs have two types of partition spaces:

- HSM administrative partition - where HSM-wide policies are set and changed, application partitions are created/destroyed, HSM firmware and capabilities are updated, etc.
- Application partition - where cryptographic operations are performed by your applications

Starting with SafeNet HSM firmware version 6.22.0, the ability to have an independent Security Officer per partition was implemented, which results in some changes from previous handling. To distinguish the different styles of partition we will call them "legacy" and "PPSO" application partitions. The options, when running SafeNet HSM Client software at the most current release are:

| HSM firmware version | PPSO Capability applied? | Ownership/oversight of partition (type) | Commands visible in lunacm when this HSM partition is the currently selected slot |
|---|---|---|---|
| <6.22.0 | cannot | legacy (see note 1) -<br>• HSM SO has full ownership of application partition and controls the application throughout its life | All commands are as they were before SafeNet HSM release 6.0 and firmware 6.22.0 |
| >=6.22 | no | legacy option (see note 2) -<br>• HSM SO has full ownership of application partition and controls the application throughout its life | lunacm HSM and partition login commands and others are replaced by "role" commands; some other commands have new options/parameters |
| >=6.22 | yes | PPSO option (see note 2) -<br>• an application partition has its own SO (which is the optional newer way to configure a new application partition)<br>• the HSM SO can create or delete the partition, but has no visibility or control in the partition through its life; complete separation of roles | lunacm HSM and partition login commands, and others, are replaced by "role" commands; some other commands have new options/parameters |
| Note 1 - No choice. With older firmware, only legacy-style partition management is available. | | | |
| Note 2 - With firmware 6.22.0 and newer, you can choose to create a partition to be owned/controlled by the HSM SO (legacy), or you can choose to create a partition to be owned and managed by its own SO (the PPSO option, invoked | | | |

| HSM firmware version | PPSO Capability applied? | Ownership/oversight of partition (type) | Commands visible in lunacm when this HSM partition is the currently selected slot |
|---|---|---|---|
| when you specify "slot" while creating a partition in lunacm, or when you specify "haspso" while creating a partition in lunash). | | | |

To summarize, until firmware 6.22 (or newer) version of SafeNet HSM receives FIPS validation, and becomes the default version shipping from the factory, you could have a new SafeNet HSM, or one that you already owned, at a firmware version older than 6.22.0. If you install newer SafeNet HSM Client, the included lunacm utility version is capable of supporting both the older command set or the newer command set, depending on the HSM firmware of the currently selected slot. That is, if you have multiple SafeNet HSMs in, or connected to, your SafeNet HSM Client host, which could include:

- internally installed SafeNet PCIe HSM,
- USB-connected SafeNet USB HSM, or
- network (NTLS- or STC-connected) SafeNet Network HSM partitions,

you could see different available command sets as you switch slots in lunacm, depending on the firmware version in the currently selected slot.

The high-level steps are summarized below, to go from a new or factory reset HSM to having a configured application partition, ready for keys and objects and cryptographic operations. Normally, each set of actions would be performed by a different person with different responsibilities.

## As the HSM Administrator or SO

1. Select/set the slot (if you have more than one HSM slot on your host).
2. Initialize the HSM; create the SO role and the cloning domain for the HSM's administrative partition (see "HSM Initialization and Zeroization" on page 1).
3. Log into the administrative partition, as SO.
4. Create the empty application partition.

## As the application partition Security Officer

5. Select/set the slot to the newly created application partition.
6. Initialize the SO role and the cloning domain for the application partition.
7. Log into the application partition as SO.
8. Initialize the Crypto Officer role.
9. Log out.

## As the application partition Crypto Officer

10. Select/set the slot to the application partition.
11. Log into the application partition as Crypto Officer.
12. Initialize the Crypto User role.

## Next step

**Note:** Before you begin configuring and initializing a PED-authenticated SafeNet HSM, we strongly urge that you familiarize yourself with the pages at "PED Authentication" on page 1.

Your responses to PED prompts are required during many of the steps. Most of the PED-prompt sequences require decisions that have serious implications for ongoing use of your HSM. PED operations are subject to timeout restrictions for security reasons, meaning that, if your selections and actions are not prompt, the PED will quit the current sequence. In the event of a timeout, you must reissue the HSM command that called the PED.

For PED-authenticated SafeNet USB HSM and SafeNet PCIe HSM, the first step is to initialize the partition; see "HSM SO Configures PED-authenticated Partition with SO, Local to Client" on page 65.

For Password-authenticated SafeNet USB HSM and SafeNet PCIe HSM, the first step is to initialize the partition; see "HSM SO Configures Password-authenticated Partition with SO, Local to Client" on page 45.

# Overview - Configure a Password-Authenticated Application Partition

You have already initialized and configured your password-authenticated SafeNet 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. You will choose between instructions for creating and configuring a legacy-style partition (owned by the HSM Security Officer) or a Per-Partition SO style partition (owned by its own separate Security Officer and largely invisible to the HSM's SO).

## High-Level Configuration Steps

1. Create a partition on the HSM, as described in "Create a Legacy Password-authenticated Application Partition " below.
2. Change the partition policies, if desired, as described in "Setting SafeNet PCIe HSM Partition Policies [Optional] " on page 52

# Legacy-style Application Partition

"Legacy", in this context, is just a name we use to indicate that an application partition has the characteristic common to SafeNet HSMs for many years, of being owned and managed by the HSM's Security Officer. Creating and configuring that type of partition is discussed in the following sections.

"Per-Partition SO" partitions have their own instruction path, later in this chapter.

# Create a Legacy Password-authenticated Application Partition

This section is HSM Partition setup for SafeNet HSM with Password Authentication. The activities in this section are required in two circumstances.

- if you just prepared the SafeNet HSM for the first time and must now create your first application Partition, or
- if you have deleted or zeroized an HSM Partition and wish to create a new one to replace it.

## About HSM Partitions on the Initialized HSM

At this point, SafeNet HSM should already have its Security Officer assigned by "Initializing a Password Authenticated HSM" on page 14.

Within the HSM, a separate cryptographic workspaces must be created. A workspace, or Partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a User who presents the proper authentication is allowed to see the Partition and to work with its contents. That User and authentication can be separate from the Security Officer identity.

In this section, you will:

- Create an HSM Partition
- Set HSM Partition Policies (Optional)

## First, Login as HSM Security Officer

1. To create HSM Partitions, you must login to the SafeNet HSM as Security Officer.

   For an HSM with firmware older than version 6.22.0, at the lunacm:> prompt, type:

   ```
   lunacm:> hsm login -password <your_password>
   ```

   For an HSM with firmware at version 6.22.0 or newer, at the lunacm:> prompt, type:

   ```
   lunacm:> role login -name SO -password <your_password>
   ```

   Authenticate as Security Officer by supplying the appropriate SO password. The password must be exactly as the HSM expects it, including proper use of uppercase/lowercase.

   > **CAUTION:** If you fail three consecutive login attempts as Security Officer, the HSM is zeroized and cannot be used as-is — it must be re-initialized. Zeroizing renders all key material unrecoverable.
   >
   > Please note that the SafeNet HSM must actually receive some information before it logs a failed attempt, so if you just press [Enter] without typing a password, that is not logged as a failed attempt. Also, when you successfully log in, the counter is reset to zero.

   If you are not sure that you are currently logged in as Security Officer, type the command ‘`hsm showinfo`’.
   For HSMs with older firmware, the item "SO Status ->" will say either "Logged in" or "Not logged in".
   For HSMs with firmware 6.22.0 or newer, the item "Role status -->" will say "none logged in", or "SO logged in".

## Second, Create the Partition

2. At the lunacm:> prompt, type:

   ```
   lunacm:> partition create

           Option -password was not supplied.  It is required.

           Enter the password: ********

           Re-enter the password: ********

           Option -domain was not specified.  It is required.

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

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

   Command Result : No Error

   lunacm:> partition login

           Option -password was not supplied.  It is required.

           Enter the password: ********

   Command Result : No Error
   ```

```
lunacm:>
```

If an error occurs, perhaps you have requested a too-short password. The password must be at least eight characters in length unless the SO sets a different minimum.

### Alternate partition dialog

When you first create a partition on a newly initialized HSM, the HSM goes immediately to the partition setup, as requested.

However, if you have previously created a partition on this HSM - and not initialized since then - the HSM detects that a valid partition is present and warns you that 'partition create' operation is about to destroy/overwrite that existing partition. It gives you the opportunity to back out of the operation and investigate, in case you are unsure of the status.

```
lunacm:> partition create

        Option -password was not supplied.  It is required.

        Enter the password: ********

        Re-enter the password: ********

        Option -domain was not specified.  It is required.

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

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

        The existing Partition 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:>
```

## Third, Set/Change Partition Policies [Optional]

3. View the partition information, including Capabilities and Policies, to see if you need to change anything. Type:

```
lunacm:> partition showpolicies
        Partition Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
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
14: Enable PED use without challenge : 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
```

```
19: Max non-volatile storage space : 3
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
30: Enable Remote Authentication : 1
        Partition Policies
0: Allow private key cloning : 0
1: Allow private key wrapping : 0
2: Allow private key unwrapping : 1
3: Allow private key masking : 0
4: Allow secret key cloning : 0
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
14: Challenge for authentication not needed : 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
19: Max non-volatile storage space : 3
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
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
```

As an example of a change, you could type:

```
lunacm:> partition changePolicy -policy 16 -value 0
```

This would have the effect of switching on RSA blinding.

## Where to go next?

Having set up your SafeNet HSM, you want to use it.

Either you have created an application of your own that can make use of an HSM, or you are using an existing third-party software. Examples might be Microsoft server applications like Certificate Services, IIS, ISA, RMS or others, which can perform their cryptographic functions in software, using local computer resources (CPU, memory, and hard disk) with their inherent security issues, or which can be configured to make use of an HSM.

If you are using one of the indicated Microsoft products, you will need to install the SafeNet CSP software and then install the server application, or else re-configure an existing installation to make use of SafeNet CSP (which provides the bridge between the application and the SafeNet HSM).

On 64-bit Windows systems, you have the option to use Microsoft's CNG (replaces CAPI), and to use our KSP provider instead of CSP.

Another option is a Java-based application, in which case you should install the SafeNet JSP, which comes with Javadocs and sample code.

# PPSO-style Application Partition

"PPSO", in this context, indicates that we are relieving the HSM's Security Officer of the duties of owning and managing the application partition, and instead creating an independent, partition-level Security Officer in charge of only the one application partition. Creating and configuring that type of partition is discussed in the following sections.

"Legacy" partitions have their own instruction path, earlier in this chapter.

## HSM SO Configures Password-authenticated Partition with SO, 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 HSM supporting the creation of a partition with its own Security Officer. These instructions assume a SafeNet HSM installed locally to the host computer, where SafeNet HSM Client software is installed, and where administrative access to the HSM is carried out via the *lunacm* tool.

You will need:

- An HSM that has firmware 6.22.0, or later, and the Per-Partition SO capability installed.

> **Note:** If you have an existing legacy partition that shares the HSM SO as its administrator, it cannot be directly turned into a partition that has its own SO. You will need to back up any contents, delete the partition, and re-create with an application partition SO.

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 ->                0
        Tunnel Slot Id ->         1
        Label ->
        Serial Number ->          150022
        Model ->                  K6 Base
        Firmware Version ->       6.22.0
        Configuration ->          Luna HSM Admin Partition  Signing With Cloning Mode
        Slot Description ->       Admin Token Slot
        HSM Configuration ->      Luna HSM Admin Partition (Password)
        HSM Status ->             OK

        Slot Id ->                2
        HSM Label ->              myG5
        HSM Serial Number ->      701312
        HSM Model ->              G5Base
        HSM Firmware Version ->   6.10.1
        HSM Configuration ->      SafeNet USB HSM (Password) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 0


Command Result : No Error

lunacm:>
```

The output shows that the host computer contains a SafeNet PCIe HSM at the desired firmware version, as slot 0, and a SafeNet USB HSM with legacy firmware as slot 2 . Both are Password-authenticated. The current slot is the SafeNet PCIe HSM, so all commands are directed to that HSM. The positions could be reversed, with the SafeNet USB HSM as the selected HSM, and having firmware 6.22.0 (or newer). The actions are the same.

```
lunacm:> hsm showinfo

        Partition Label ->
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> K6 Base
        Partition Serial Number -> 150022
        Partition Status -> Zeroized
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED

        Slot Id -> 0
        Tunnel Slot Id -> 1
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->

        Partition OUID: Not Available
        Partition Storage:
                Total Storage Space:  0
                Used Storage Space:   0
                Free Storage Space:   0
                Object Count:         0
                Overhead:             2156
        Firmware Version -> 6.22.0
        Rollback Firmware Version -> 6.21.0
        RPV Initialized -> Not Available / Not Supported
        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   0
                Number of Partitions: 0

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

        License Count -> 8
                1. 621000026-000 K6 base configuration
                1. 620127-000 Elliptic curve cryptography
                1. 620114-001 Key backup via cloning protocol
                1. 621010089-001 Enable remote PED capability
                1. 621000021-001 Performance level 15
```

```
               1. 621000079-001 Enable Small Form Factor Backup

Command Result : No Error

lunacm:>
```

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

1. Initialize the HSM.
   Type **hsm init -label** <a label>

   ```
   lunacm:> hsm init -label mylunapci

           You are about to initialize the HSM.
           All contents of the HSM will be destroyed.
           All roles will be destroyed.
           The domain will be destroyed.

           Are you sure you wish to continue?

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


   Command Result : No Error

   lunacm:>
   ```

> **Note:** PKCS slot numbering starts at zero.
>
> At least 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. Before the admin partition is initialized, the placeholder is at slot 0. After the admin partition is initialized, it takes a higher slot number and leaves the placeholder for a future application partition.
>
> SafeNet HSMs and libraries uphold PKCS standards, which require that the slot number must not change during the current session. Therefore, in order for the HSM administrative slot to become slot 1 in this example, and leave room at slot 0 for creation of an application partition, you must restart the session. You can keep lunacm open and run the command **clientconfig restart**, or you can exit lunacm (which closes the session) after initializing the HSM administrative partition and then relaunch lunacm. Either of those actions starts a new session with the slots renumbered. Either of those actions sets the current slot back to the lowest slot (if that was not the selected slot before you restarted or exited and relaunched).
>
> Also, be aware that it is possible to override the default numbering and force the starting slot number by modifying the config file.

2. Exit and re-launch lunacm.

   ```
   lunacm:> exit

   C:\Program Files\SafeNet\LunaClient>lunacm
   ```

```
LunaCM V2.3.3 - Copyright (c) 2006-2013 SafeNet, Inc.

        Available HSMs:

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mylunapci
        Serial Number ->        150022
        Model ->                K6 Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition  Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (Password)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5
        HSM Serial Number ->    701312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.1
        HSM Configuration ->    SafeNet USB HSM (Password) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 1

lunacm:>
```

3. Log in as the HSM Administrator:
   Type **role login -name Administrator**

```
lunacm:> role login -name Administrator



Command Result : No Error

lunacm:>
```

4. Create an application partition, intended to have its own SO, by specifying the "-slot" parameter. Note that the HSM administrative partition is always the highest numbered slot, therefore it becomes slot 1, leaving slot 0 available for the application partition that you are creating.
   Type **partition create -slot** <slot number>

```
lunacm:> par create -slot 0

Command Result : No Error

lunacm:> slot list
```

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

```
lunacm:> slot list

        Slot Id ->              0
        Tunnel Slot Id ->       2
        Label ->
        Serial Number ->        349297122738
        Model ->                K6 Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna User Partition With SO  Signing With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mylunapci
        Serial Number ->        150022
        Model ->                K6 Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition  Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (Password)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5
        HSM Serial Number ->    701312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.1
        HSM Configuration ->    SafeNet USB HSM (Password) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 1


Command Result : No Error

lunacm:>
```

6. The HSM SO now informs the intended application partition SO
   a. the newly created, empty application partition is ready,
   b. how to access it.

This concludes the HSM SO's actions for a partition with its own SO. 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 PPSO Partition" below.

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

These instructions assume a Password-authenticated SafeNet HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer (see previous steps by HSM SO "HSM SO

Configures Password-authenticated Partition with SO, Local to Client" on page 45).

### Step 1: Initialize the Partition SO role

1. Set the active slot to the created, uninitialized, application partition.
   Type **slot set -slot** <slot number>

   ```
   lunacm:> slot set -slot 0

           Current Slot Id:    0     (Luna User Slot 6.22.0 (Password) Signing With Cloning
   Mode)


   Command Result : No Error

   lunacm:>
   ```

2. Initialize the application partition, to create the partition's Security Officer (SO).
   Type **partition init -label** <a label>

   ```
   lunacm:> par init -label ppsopar

           You are about to initialize the partition.
           All partition objects 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:>
   ```

### Step 2: Initialize the Crypto Officer role

1. The SO of the application partition can now assign the first operational role within the new partition.
   Type **role login -name Partition SO**

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


   Command Result : No Error

   lunacm:>
   ```

2. Type **role init -name Crypto Officer**

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



   Command Result : No Error

   lunacm:>
   ```

3. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.
   Type **role logout**

```
lunacm:> role logout

Command Result : No Error

lunacm:>
```

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-Auth PPSO Partition " below.

# Initialize the Crypto User Role on a PW-Auth PPSO Partition

These instructions assume

- a Password-authenticated SafeNet HSM has been initialized,
- an application partition has been created,
- a Crypto Officer has been created for the partition, and
- 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 PPSO Partition" on page 49.

As Crypto Officer, you can do the following:

- 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.
   Type **slot set -slot** <slot number>

```
lunacm:> slot set -slot 0

        Current Slot Id:    0     (Luna User Slot 6.22.0 (PW) Signing With Cloning Mode)


Command Result : No Error

lunacm:>
```

2. Log in as the Crypto Officer.
   Type **role login -name Crypto Officer**

```
lunacm:> role login -name Crypto Officer -password $3cr3t
```

```
Command Result : No Error

lunacm:>
```

3. Create the Crypto User.
   Type **role init -name Crypto User**

```
lunacm:> role init -name Crypto User -password 0ther$ecret


Command Result : No Error

lunacm:>
```

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.

# Setting SafeNet PCIe HSM Partition Policies [Optional]

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.

## Example policy change procedure

In this example, we show the initial values of the Partition Capabilities and their corresponding Policies, then we change one Policy, and show the values again.

```
lunacm:> partition showinfo

        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        User Status->                  Not Logged In
        Crypto Officer Failed Logins-> 0
        Crypto User Failed Logins->    0
        User Flags ->
                CONTAINER_KCV_CREATED
        User OUID: 6e000000e400000056f60600

        User Storage:
                Total Storage Space:  2094996
                Used Storage Space:   0
                Free Storage Space:   2094996
                Object Count:         0

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


        License Count -> 9
                1. 0009-020 Test K6 Base Config - 9-20
                2. 620109-000 Test K3 FIPS3 Update - 620109
                3. 0009-030 Test K3 HSM Cloning Update - 000009-030
                4. 620127-000 Test K3 ECC Update - 620127
                5. 0009-025 Test K3 External MTK Update 2 - 000009-025
                6. 620111-000 Test K3 Performance 600 Update - 620111
                7. 0009-015 Test K3 Remote Ped Update - 000009-015
                8. 620124-000 Test K3 Partitions 20 Update - 620124
                9. 620114-000 Test K3 Cloning Update - 620114

Command Result : No Error
lunacm:>


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
                14: Enable PED use without challenge : 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 : 1
                23: Enable auto-activation : 1
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 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
                14: Challenge for authentication not needed : 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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

In the example above, we change the maximum number of consecutive failed login attempts that is permitted on the Partition.
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.

```
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
                14: Enable PED use without challenge : 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 : 1
                23: Enable auto-activation : 1
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 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
                14: Challenge for authentication not needed : 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 :9   <--
                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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

Note in the above example that HSM Capability "20: Max failed user logins allowed : 10" still has a value of 10 (meaning that 10 is as many failed Partition login attempts as can be permitted), but the associated Policy "20: Max failed user logins allowed : **9**" now has a value of 9 - meaning that the 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; that is, the SO has increased the security on the partition.

# Overview - Configure a PED-Authenticated Application Partition

You have already initialized and configured your PED-authenticated SafeNet 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. You will choose between instructions for creating and configuring a legacy-style partition (owned by the HSM Security Officer) or a Per-Partition SO style partition (owned by its own separate Security Officer and largely invisible to the HSM's SO).

## High-Level Configuration Steps

1. Create a partition on the HSM, as described in "Create a Legacy Password-authenticated Application Partition " on page 41.
2. Change the partition policies, if desired, as described in "Setting SafeNet PCIe HSM Partition Policies [Optional]" on page 1.

# Legacy-style Application Partition

"Legacy", in this context, is just a name we use to indicate that an application partition has the characteristic common to SafeNet HSMs for many years, of being owned and managed by the HSM's Security Officer. Creating and configuring that type of partition is discussed in the following sections.

"Per-Partition SO" partitions have their own instruction path, later in this chapter.

# Creating a Legacy-style PED-authenticated Application Partition

This section is application Partition setup for a SafeNet HSM with PED Authentication, where the partition is to remain under the ownership of the HSM Security Officer. The activities in this section are required in two circumstances.

- if you just prepared an HSM for the first time and must now create your first application Partition, or
- if you have deleted or zeroized an application Partition and wish to create a new one to replace it.

## About Application Partitions on the Initialized HSM

At this point, the SafeNet HSM should already have its Security Officer assigned at "Initialize the HSM " on page 12.

Within the HSM, a separate cryptographic work-space must be created, for use by client applications. A workspace, or partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a User who presents the proper authentication is allowed to see the application partition and to work with its contents. That User (or Crypto Officer) and its authentication can be separate from the Security Officer identity. However, in the legacy approach, the HSM SO maintains direct authority and ability to see into the application partition.

In this section, you will:

- Create an application Partition
- Set application Partition Policies (Optional)

If your SafeNet HSM is at a version lower than 6.22.0.he commands available in lunacm are the traditional ones that have been used with SafeNet HSMs. The outcome of this sequence is the creation of a legacy-style application partition that is owned and managed by the HSM SO and does not have its own independent SO.

If your HSM firmware is at version 6.22.0 or higher, then some of the commands have changed, and are the same as those listed for creation of a PPSO application partition, in another section of this guide. That is, with the newer firmware you can use the newer commands to create either a legacy-style partition or a PPSO partition. With the pre-6.22.0 firmware, you have only the older commands, and you can create only a legacy-style partition.

"Legacy" partitions with old firmware behave slightly differently from "legacy" partitions with 6.22-and-newer firmware. In the old firmware, for SafeNet USB HSM and for SafeNet PCIe HSM, "slot list" shows only one slot, even after a partition has been created. Pre-f/w-6.22, the application partition essentially shares its slot with the HSM's administrative partition. With firmware 6.22, "slot list" shows separate:
- HSM Admin slot ( Configuration -> SafeNet HSM Admin Partition Signing With Cloning Mode )
  and
- application partition slot ( Configuration -> SafeNet User Partition, No SO Signing With Cloning Mode ).

## First, Login as Security Officer

To create HSM Partitions, you must login to the SafeNet HSM as Security Officer.

1. In a terminal window (DOS command-line window in Windows), go to the SafeNet HSM Client directory and start the lunacm utility.
2. In lunacm, if you have more than one HSM on the current host computer, set the correct slot. At the lunacm:> prompt, type:

   ```
   lunacm:> slot set slot <number of HSM administrative slot>
   ```

3. Log in as the HSM SO.

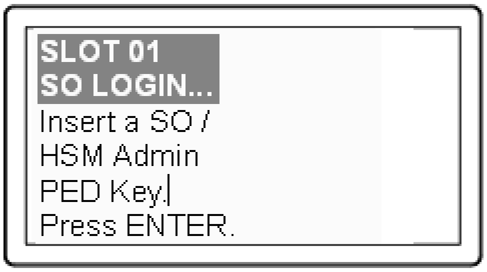
   For firmware older than 6.22.0, at the lunacm:> prompt, type:

   ```
   lunacm:> hsm login
   ```

   For firmware 6.22.0 or newer, at the lunacm:> prompt, type:

   ```
   lunacm:> role login -name Administrator
   ```

You are directed to SafeNet PED.



SLOT 01
SO LOGIN...
Insert a SO /
HSM Admin
PED Key.
Press ENTER.

Authenticate as Security Officer by supplying the appropriate HSM SO PED Key that was imprinted during the HSM initialization step. The PED might prompt you for the numeric password PED PIN that might optionally have been assigned to the HSM SO PED Key. SafeNet PED provides the HSM SO authentication secret to the SafeNet HSM.

⚠ **CAUTION:** If you fail three consecutive login attempts as Security Officer, the HSM is zeroized and cannot be used as-is — it must be re-initialized. Zeroizing destroys all key material.

Actions that are flagged as bad login attempts on a PED-authenticated HSM are:

- offering a PED Key that has the correct color/authent-type, but that carries a wrong authentication secret for the current HSM,

- offering a PED Key that contains the correct secret, but just pressing [Enter] on the PED keypad, with no digits, when a PED PIN was expected,

- offering a PED Key that contains the correct secret, but typing any numbers when no PED PIN had previously been set).

Please note that the SafeNet HSM must actually receive some information before it logs a failed attempt, so actions that would not trigger the bad-login counter might include:

-if you just press [Enter] on the PED keypad without a PED Key inserted, or

- if you insert a wrong-color* PED Key and press [Enter],

those are not logged as failed attempts.

When you successfully login, the counter is reset to zero.

(*Wrong color means that the PED Key that you present has been imprinted with an authentication secret for a different function than is currently requested - so inserting a cloning domain (red) key when a blue key is requested is not a bad login attempt; it's just an inconvenience.)

If you are not sure that you are currently logged in as Security Officer, perform an '`hsm login`'. Either you will be directed to the PED to present the blue PED Key and log in, or you will be told that the SO is already logged in.

## Second, Create the Partition

1. Have the SafeNet PED connected and ready (in Local mode and "Awaiting command...").
2. Have a blank, black-labeled PED Key (or a previously imprinted PED Key that you wish to share, or to overwrite) ready to insert into the USB connector at the top of the PED.
3. Run the "partition create" command.

   The following is an example of initialization dialog, with PED interactions inserted to show the sequence of events.

   For firmware older than 6.22.0, type:

   ```
   lunacm:> partition create
   ```

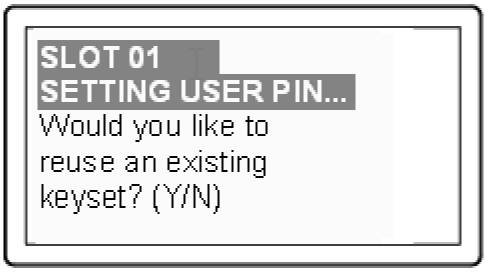
   For firmware 6.22.0 or newer, type:

   ```
   lunacm:> partition create -label mylegacypar

   The existing Partition will be destroyed.
   Are you sure you wish to continue?
   ```

```
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Please attend to the PED.
Command Result : No Error
        Please attend to the PED.
```

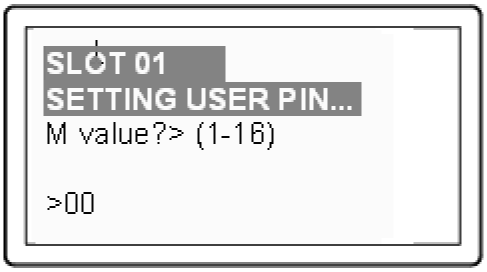
4. SafeNet PED asks preliminary setup questions, prior to imprinting the first black Partition Crypto Officer PED Key.



SLOT 01
SETTING USER PIN...
Would you like to
reuse an existing
keyset? (Y/N)

Respond "Yes" if you have a key from another HSM partition with a partition Owner / Crypto Officer ID already imprinted on it, that you wish to share/reuse.
Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve.
(See "Shared or Group PED Keys" on page 1 for more detail)

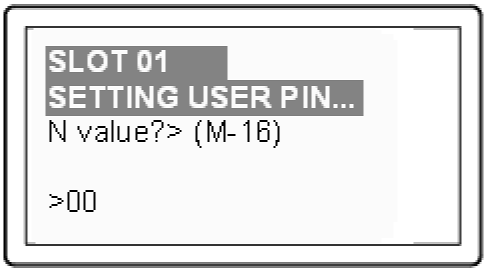
5. The PED requests values for :



SLOT 01
SETTING USER PIN...
M value?> (1-16)

>00

and

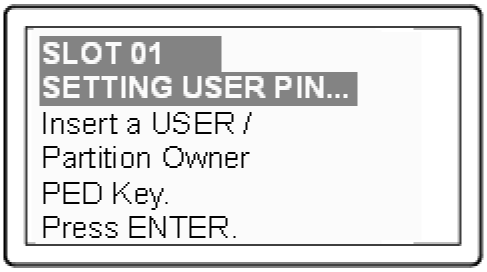


SLOT 01
SETTING USER PIN...
N value?> (M-16)

>00

(enter "1" for both, unless you wish to invoke MofN split-secret, multi-person access control, "Using MofN" on page 1).

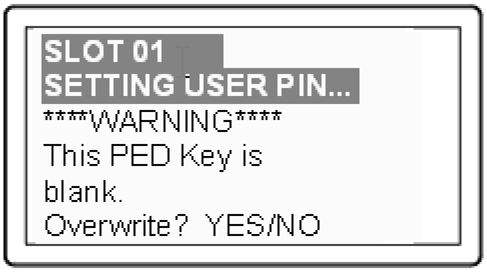
6. The PED then demands the black Owner PED key with the message



```
SLOT 01
SETTING USER PIN...
Insert a USER /
Partition Owner
PED Key.
Press ENTER.
```

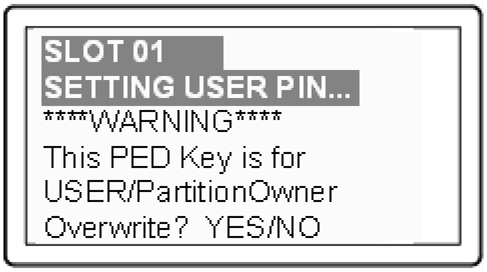
Insert the intended black HSM Partition Owner PED key [ of course, the unlabeled PED Key is generically black - we suggest that you apply the appropriate color sticker either immediately before or immediately after imprinting the key; before, just to ensure it gets done, or after, as a helpful indicator as to which ones are imprinted (with which secret), and which ones still blank ] and press [Enter]. A unique Partition Owner / Crypto Officer PIN is to be imprinted on both the PED key and the HSM Partition.

7. The PED continues with one or the other of these responses:



```
SLOT 01
SETTING USER PIN...
****WARNING****
This PED Key is
blank.
Overwrite?  YES/NO
```

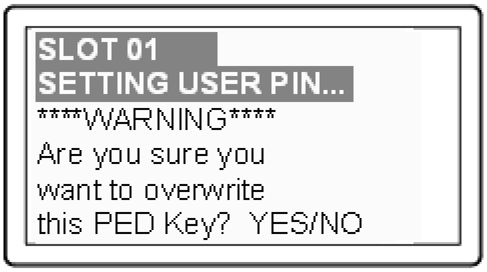
**OR**



```
SLOT 01
SETTING USER PIN...
****WARNING****
This PED Key is for
USER/PartitionOwner
Overwrite?  YES/NO
```

Decide whether this should be a group PED Key (see "What is a Shared or Group PED Key?" ), press [YES] or [NO] on the PED keypad, and press [Enter].

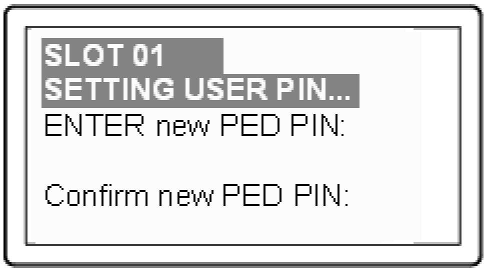
8. This is potentially serious business (if you unintentionally overwrite a PED Key that is needed for other purposes), so SafeNet PED asks one more time if you truly intend to overwrite the key's content.



SLOT 01
SETTING USER PIN...
****WARNING****
Are you sure you
want to overwrite
this PED Key? YES/NO

Press [YES] or [NO] on the PED keypad, and press [Enter].

9. Next, you are asked to provide a PED PIN (optional, see "What is a PED PIN?" — can be 4-to-48 digits, or can be *no* digits if a PED PIN is not desired).

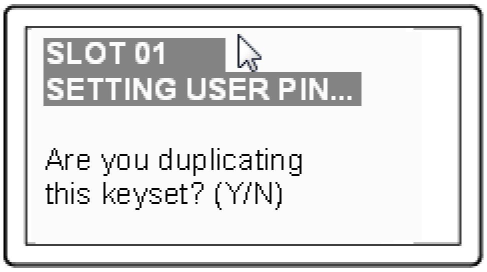


SLOT 01
SETTING USER PIN...
ENTER new PED PIN:

Confirm new PED PIN:

You must press [Enter] to inform the PED that you are finished entering PED PIN digits, *or* that you have decided **not** to use a PED PIN (no digits entered).
When you provide a PED PIN – even if it is the null PIN (by just pressing [Enter] with no digits) – the PED requests it a second time, to ensure that you entered it correctly, as you intended.
Press [ENTER] again.

10. You are then prompted



SLOT 01
SETTING USER PIN...

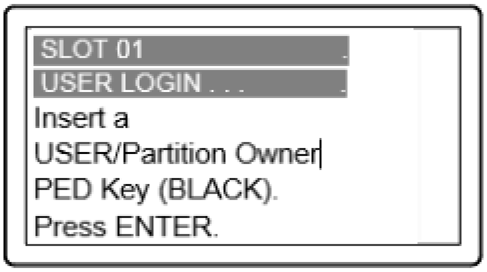
Are you duplicating
this keyset? (Y/N)

See "What is a duplicate PED Key?".
Respond "No", if you want the PED to imprint just the one black HSM Admin PED Key and go on to the next step in creation of the application Partition.
Respond "Yes", if you want the PED to imprint the first black key and then ask for more black PED Keys, until you have imprinted (duplicated) as many as you wish.

You should probably make at least one copy of this key as a backup. Some security regimes would have a working copy for on-site storage and another copy for off-site backup. As long as you continue to say "Yes" and present more keys to be imprinted, SafeNet PED continues to make copies of the current PED Key.

When you are done, say "No".

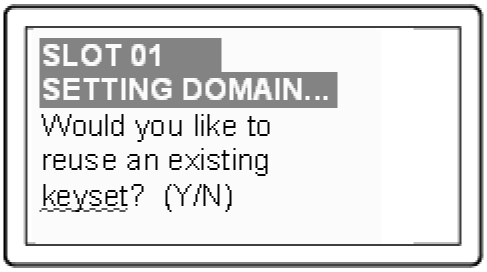
11. Having created the black key User or Crypto Officer, the HSM now needs you to log in as that identity, in order to create or imprint a cloning domain for the partition. The PED prompts:



SLOT 01
USER LOGIN . . .
Insert a
USER/Partition Owner
PED Key (BLACK).
Press ENTER.

Leave the black key inserted, and press Enter.

12. The PED inquires if you intend to reuse a previously imprinted red Domain PED Key.



SLOT 01
SETTING DOMAIN...
Would you like to
reuse an existing
keyset? (Y/N)

Respond "Yes" if you have a key from another HSM partition with a cloning domain ID already imprinted on it, that you wish to share/reuse to allow the two partitions to clone to each other, or to-and-from the same backup. Respond "No" if you have a fresh, never-imprinted key, or if you have a key previously imprinted with an ID that you do not wish to preserve.

13. You now have a legacy application partition (owned and ultimately controlled by the HSM SO) with a User or Crypto Officer to manage it, and to determine when it is open for use by applications (activated), and when not. The client applications need a way to authenticate to the application partition that does not involve your presence with PED and PED Key all the time. For this purpose, you request the HSM to create a challenge secret text-string, suitable for use by applications.
Log in as the HSM SO.

For firmware older than 6.22.0, type:

```
lunacm:> hsm login
```

For firmware 6.22.0 or newer, type:

```
lunacm:> role login -name Administrator
```

14. Create the challenge secret text string:

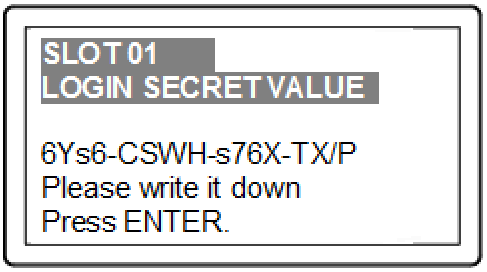
```
lunacm:> partition createChallenge

        Please attend to the PED.

Command Result : No Error

lunacm:>
```

The PED screen shows a generated string of characters that you must record accurately and promptly.



SLOT 01
LOGIN SECRET VALUE

6Ys6-CSWH-s76X-TX/P
Please write it down
Press ENTER.

Because most problems with a challenge secret seem to result from ambiguous or indecipherable handwriting, we strongly suggest that you record down the string in a text editor.

**Note:** The dashes/hyphens shown between blocks of characters, in the illustration above, are NOT part of the challenge secret. They are added by the PED, simply for readability while you are recording. When you provide the string for your applications to use, be sure to remove the hyphens.

Alternatively, you can change the challenge secret to something more friendly :

```
lunacm:> partition changePw -newpw Thisisa$3cr3t -oldpw 6Ys6CSWHs76XTX/P
        Please attend to the PED.
Command Result : No Error
lunacm:>
```

Optionally, go to "Setting SafeNet PCIe HSM Partition Policies [Optional]" on page 73 to adjust behavioral and security parameters for the newly created partition.

## Where to go next?

Having set up your SafeNet HSM, you want to use it.

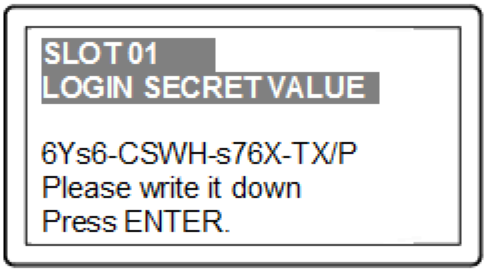
Either you have created an application of your own that can make use of an HSM, or you are using an existing third-party software. Examples might be Microsoft server applications like Certificate Services, IIS, ISA, RMS or other applications from other vendors. By default, such applications can perform their cryptographic functions in software, using local computer resources (CPU, memory, and hard disk) with their inherent security issues, or they can be configured to make use of an HSM like the SafeNet HSM.

If you are using one of the indicated Microsoft products, you will need to install the SafeNet CSP / KSP software and then install the server application, or else re-configure an existing installation to make use of SafeNet CSP (for CAPI environment) or SafeNet KSP for CNG environment, to provide the bridge between the application and the SafeNet HSM).

Another option is a Java-based application, in which case you should install the SafeNet JSP, which comes with Javadocs and sample code.

## Record the Partition Client Password (PED-Auth HSMs)

The PED now generates and displays the Client Password (login secret), by which Clients will later authenticate themselves to this HSM Partition.



SLOT 01
LOGIN SECRET VALUE

6Ys6-CSWH-s76X-TX/P
Please write it down
Press ENTER.

Record the Login Secret Value from the PED screen – write it down legibly – because it will never be shown again. This is the HSM Partition password, used to authenticate Client applications that wish to use the HSM Partition on the SafeNet Network HSM.

**Note:** It might be best to use a text editor, because the majority of errors tend to occur when reading hand-written values. The password/challenge secret is case-sensitive.

**Note:** The PED times out after eight minutes. You must complete recording the password and press the ENTER button before time-out occurs.

When you press [ENTER] on the PED keypad, control returns to the command prompt, where a success message is displayed:

```
'partition create' successful
```

At the same time, SafeNet PED goes back to "Awaiting command...".

Next you might need to adjust the Partition Policy settings for the new Partition. (Optional see "Partition Policies" )

Otherwise, see "Creating a Network Link Between the Client and the Partition" on page 1.

# PPSO-style Application Partition

"PPSO", in this context, indicates that we are relieving the HSM's Security Officer of the duties of owning and managing the application partition, and instead creating an independent, partition-level Security Officer in charge of only the one application partition. Creating and configuring that type of partition is discussed in the following sections.

"Legacy" partitions have their own instruction path, earlier in this chapter.

## HSM SO Configures PED-authenticated Partition with SO, 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 HSM supporting the creation of a partition with its own Security Officer. These instructions assume a SafeNet HSM installed locally to the host computer, where SafeNet HSM Client software is installed, and where administrative access to the HSM is carried out via the lunacm utility.

You will need:

- An HSM that has firmware 6.22.0, or later, and the Per-Partition SO capability installed.
- SafeNet PED and PED Keys with labels. These instructions assume that your SafeNet PED is locally connected. 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.

> **Note:** If you have an existing legacy partition that shares the HSM SO as its administrator, it cannot be directly turned into a partition that has its own SO. You will need to back up any contents, delete the partition, and re-create with an application partition SO.

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 ->                0
        Tunnel Slot Id ->         1
        Label ->
        Serial Number ->          150022
        Model ->                  K6 Base
        Firmware Version ->       6.22.0
        Configuration ->          Luna HSM Admin Partition  Signing With Cloning Mode
        Slot Description ->       Admin Token Slot
        HSM Configuration ->      Luna HSM Admin Partition (PED)
        HSM Status ->             OK

        Slot Id ->                2
        HSM Label ->              myG5
        HSM Serial Number ->      701312
        HSM Model ->              G5Base
        HSM Firmware Version ->   6.10.1
        HSM Configuration ->      SafeNet USB HSM (PED) Signing With Cloning Mode
        HSM Status ->             OK



        Current Slot Id: 0


Command Result : No Error

lunacm:>
```

The output shows that the host computer contains a SafeNet PCIe HSM at the desired firmware version, as slot 0, and a SafeNet USB HSM with legacy firmware as slot 2 . Both are PED-authenticated. The current slot is the SafeNet PCIe HSM, so all commands are directed to that HSM.

```
lunacm:> hsm showinfo

        Partition Label ->
        Partition Manufacturer -> Safenet, Inc.
        Partition Model -> K6 Base
        Partition Serial Number -> 150022
        Partition Status -> Zeroized
        Token Flags ->
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Slot Id -> 0
        Tunnel Slot Id -> 1
        Session State -> CKS_RW_PUBLIC_SESSION
        Role Status ->   none logged in
        Token Flags ->

        Partition OUID: Not Available
        Partition Storage:
                Total Storage Space:  0
                Used Storage Space:   0
                Free Storage Space:   0
                Object Count:         0
                Overhead:             2156
        Firmware Version -> 6.22.0
        Rollback Firmware Version -> 6.21.0
        RPV Initialized -> Not Available / Not Supported
        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   0
                Number of Partitions: 0

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

        License Count -> 8
                1. 621000026-000 K6 base configuration
                1. 620127-000 Elliptic curve cryptography
                1. 620114-001 Key backup via cloning protocol
                1. 620109-000 PIN entry device (PED) enabled
                1. 621010358-001 Enable a split of the master tamper key to be stored externally
                1. 621010089-001 Enable remote PED capability
                1. 621000021-001 Performance level 15
                1. 621000079-001 Enable Small Form Factor Backup

Command Result : No Error

lunacm:>
```

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

Have PED Keys and labels ready and have a SafeNet PED connected to the HSM, and set to Local Mode.

1. Initialize the HSM.
   Type **hsm init -label** <a label>

```
lunacm:> hsm init -label mylunapci

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.
        All roles will be destroyed.
        The domain will be destroyed.

        Are you sure you wish to continue?

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

        Please attend to the PED.
```

   Respond to SafeNet PED prompts...

```
Command Result : No Error

lunacm:>
```

> **Note:** PKCS slot numbering starts at zero.
>
> At least 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. Before the admin partition is initialized, the placeholder is at slot 0. After the admin partition is initialized, it takes a higher slot number and leaves the placeholder for a future partition.
>
> SafeNet HSMs and libraries uphold PKCS standards, which require that the slot number must not change during the current session. Therefore, in order for the HSM administrative slot to become slot 1 in this example, and leave room at slot 0 for creation of an application partition, you must exit lunacm (which closes the session) after initializing the HSM administrative partition and then relaunch lunacm, which starts a new session with the slots renumbered.
>
> Also, be aware that it is possible to override the default numbering and force the starting slot number.

2. Exit and re-launch lunacm.

```
lunacm:> exit

C:\Program Files\SafeNet\LunaClient>lunacm

LunaCM V2.3.3 - Copyright (c) 2006-2013 SafeNet, Inc.


        Available HSMs:

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mylunapci
        Serial Number ->        150022
        Model ->                K6 Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition  Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5
        HSM Serial Number ->    701312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.1
        HSM Configuration ->    SafeNet USB HSM (PED) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 1

lunacm:>
```

3. Log in as the HSM Administrator:
   Type **role login -name Administrator**

```
lunacm:> role login -name Administrator

        Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error

lunacm:>
```

4. Create an application partition, intended to have its own SO, by specifying the "-slot" parameter. Note that the HSM administrative partition is always the highest numbered slot, therefore it becomes slot 1, leaving slot 0 available for the application partition that you are creating.
   Type **partition create -slot** <slot number>

```
lunacm:> par create -slot 0

Command Result : No Error

lunacm:> slot list
```

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

```
lunacm:> slot list

        Slot Id ->              0
        Tunnel Slot Id ->       2
        Label ->
        Serial Number ->        349297122738
        Model ->                K6 Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna User Partition With SO  Signing With Cloning Mode
        Slot Description ->     User Token Slot

        Slot Id ->              1
        Tunnel Slot Id ->       2
        Label ->                mylunapci
        Serial Number ->        150022
        Model ->                K6 Base
        Firmware Version ->     6.22.0
        Configuration ->        Luna HSM Admin Partition  Signing With Cloning Mode
        Slot Description ->     Admin Token Slot
        HSM Configuration ->    Luna HSM Admin Partition (PED)
        HSM Status ->           OK

        Slot Id ->              3
        HSM Label ->            myG5
        HSM Serial Number ->    701312
        HSM Model ->            G5Base
        HSM Firmware Version -> 6.10.1
        HSM Configuration ->    SafeNet USB HSM (PED) Signing With Cloning Mode
        HSM Status ->           OK



        Current Slot Id: 1

Command Result : No Error

lunacm:>
```

6. The HSM SO now informs the intended application partition SO
   a. the newly created, empty application partition is ready,
   b. how to access it.

This concludes the HSM SO's actions for a partition with its own SO. 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 "Partition SO Configures PED-authenticated PPSO Application Partition" on page 1.

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

These instructions assume a PED-authenticated SafeNet HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer (see previous steps by HSM SO "HSM SO Configures PED-authenticated Partition with SO, Local to Client" on page 65).

You will need:

- An HSM that has firmware 6.22.0, or later, and the Per-Partition SO capability installed.

- SafeNet PED and PED Keys with labels. These instructions assume that your SafeNet PED is connected locally.
- 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.

### Step 1: Initialize the Partition SO role

1. Set the active slot to the created, uninitialized, application partition.
   Type **slot set -slot** <slot number>

```
lunacm:> slot set -slot 0

        Current Slot Id:    0     (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)


Command Result : No Error

lunacm:>
```

2. Initialize the application partition, to create the partition's Security Officer (SO).
   Type **partition init -label** <a label>

```
lunacm:> par init -label ppsopar

        You are about to initialize the partition.
        All partition objects will be destroyed.


        Are you sure you wish to continue?

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

        Please attend to the PED.
```

   Respond to SafeNet PED prompts...

```
Command Result : No Error

lunacm:>
```

### Step 2: Initialize the Crypto Officer role

1. The SO of the application partition can now assign the first operational role within the new partition.
   Type **role login -name Partition SO**

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

        Please attend to the PED.

Command Result : No Error

lunacm:>
```

2. Type **role init -name Crypto Officer**

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

        Please attend to the PED.
```

Respond to SafeNet PED prompts...

```
Command Result : No Error

lunacm:>
```

3. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.
   Type **role logout**

```
lunacm:> role logout

Command Result : No Error

lunacm:>
```

At this point, the Crypto Officer, or an application using the CO's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto Officer logs in with **role login -name Crypto Officer**. However, the Crypto Officer can create, modify and delete crypto objects within the partition, in addition to merely using 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-Auth PPSO Partition " below.

# Initialize the Crypto User Role on a PED-Auth PPSO Partition

These instructions assume

- a PED-authenticated SafeNet HSM has been initialized,
- an application partition has been created,
- a Crypto Officer has been created for the partition, and
- 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 PPSO Partition" on page 69.

As Crypto Officer, you can do the following:

- 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:

- SafeNet PED and the black Crypto Officer PED Key(s) assigned to you by the SO, as well as blank PED Key(s) with labels for the Crypto User that you are about to create. These instructions assume that your SafeNet PED is locally connected. 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 PPSO application partition

1. Set the active slot to the desired application partition, where the Crypto Officer was just created.
   Type **slot set -slot** <slot number>

```
lunacm:> slot set -slot 0

        Current Slot Id:    0     (Luna User Slot 6.22.0 (PED) Signing With Cloning Mode)


Command Result : No Error

lunacm:>
```

2. Log in as the Crypto Officer.
   Type **role login -name Crypto Officer**

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

        Please attend to the PED.
```

   Respond to SafeNet PED prompts...

```
Command Result : No Error

lunacm:>
```

3. Create the Crypto User.
   Type **role init -name Crypto User**

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

        Please attend to the PED.
```

   Respond to SafeNet PED prompts...

```
Command Result : No Error

lunacm:>
```

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.

It is possible for all three of Partition SO, Crypto Officer, and Crypto User to perform their functions against a SafeNet Network HSM partition, from the same SafeNet HSM Client host computer, simply taking turns at the keyboard and the SafeNet PED. It is also possible to work from different computers, as long as any such computer is a registered user of the partition - that is, a working network trust link (NTL) connection is required for each.

In addition, if those persons and their respective SafeNet HSM Client host computers are **not** co-located, then they must arrange to manage their sharing of the Remote PED. Either

- one person must maintain the single Remote PED setup, and the others must coordinate closely with the PED-keeper when authentication to the HSM is required,

  or

- all three can have their own separate PEDs and PedServer instances, but they must coordinate with the appliance administrator to **hsm ped disconnect** any current Remote PED channel before **hsm ped connect -ip <new-ip> -port <new-port>** to establish a Remote PED session with one of the other PedServers.

## Crypto Officer or Crypto User Must Log In and 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 Crypto User**.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 "SO and CO Activate PED-authenticated PPSO Application Partition " on page 1 or "SO and CU Activate PED-authenticated PPSO Application Partition " on page 1.

# Setting SafeNet PCIe HSM Partition Policies [Optional]

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.

### Example policy change procedure

In this example, we show the initial values of the Partition Capabilities and their corresponding Policies, then we change one Policy, and show the values again.

```
lunacm:> partition showinfo

        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        User Status->                  Not Logged In
        Crypto Officer Failed Logins-> 0
        Crypto User Failed Logins->    0
        User Flags ->
                CONTAINER_KCV_CREATED
        User OUID: 6e000000e400000056f60600

        User Storage:
                Total Storage Space:  2094996
                Used Storage Space:   0
                Free Storage Space:   2094996
                Object Count:         0

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


        License Count -> 9
                1. 0009-020 Test K6 Base Config - 9-20
                2. 620109-000 Test K3 FIPS3 Update - 620109
                3. 0009-030 Test K3 HSM Cloning Update - 000009-030
                4. 620127-000 Test K3 ECC Update - 620127
                5. 0009-025 Test K3 External MTK Update 2 - 000009-025
                6. 620111-000 Test K3 Performance 600 Update - 620111
                7. 0009-015 Test K3 Remote Ped Update - 000009-015
                8. 620124-000 Test K3 Partitions 20 Update - 620124
                9. 620114-000 Test K3 Cloning Update - 620114

Command Result : No Error
lunacm:>


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
                14: Enable PED use without challenge : 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 : 1
                23: Enable auto-activation : 1
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 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
                14: Challenge for authentication not needed : 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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

In the example above, we change the maximum number of consecutive failed login attempts that is permitted on the Partition.
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.

```
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
                14: Enable PED use without challenge : 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 : 1
                23: Enable auto-activation : 1
                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
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 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
                14: Challenge for authentication not needed : 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 :9   <--
                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
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

Note in the above example that HSM Capability "20: Max failed user logins allowed : 10" still has a value of 10 (meaning that 10 is as many failed Partition login attempts as can be permitted), but the associated Policy "20: Max failed user logins allowed : **9**" now has a value of 9 - meaning that the 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; that is, the SO has increased the security on the partition.

# 3 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 (HA) Configuration and Operation" 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" on page 1 in the *Administration Guide*.