# SafeNet PCIe HSM 7.0

## Key Migration Guide

gemalto

security to be free

## Document Information

| | |
|---|---|
| **Product Version** | 7.0 |
| **Document Part Number** | 007-013576-001 |
| **Release Date** | 25 October 2016 |

## Revision History

| Revision | Date | Reason |
|---|---|---|
| A | 25 October 2016 | Initial release. |

## Trademarks, Copyrights, and Third-Party Software

### Acknowledgements

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

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

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

This product uses Brian Gladman’s AES implementation.

Refer to the End User License Agreement for more information.

## Disclaimer

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

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

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

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

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

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

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

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

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

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Gemalto

## Regulatory Compliance

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

### USA, FCC

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

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

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

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

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

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

## Canada

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

## Europe

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

# CONTENTS

# PREFACE

# About the LunaSH Command Reference Guide

This document describes how to do something (insert a brief description). It contains the following chapters:

- "Using LunaSH" on page 1
- "Lunash Commands" on page 1

This preface also includes the following information about this document:

- "Customer Release Notes" on page 1
- "Gemalto Rebranding" on page 1
- "Audience" on page 1
- "Document Conventions" on page 1
- "Support Contacts" on page 1

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

## Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. It is strongly recommended that you 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/

## 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 |

| Old product name | New product name |
|---|---|
| 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. |
| [**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. |
| {**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. |
| [**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 |

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

# 1

# Network HSM Partition (5.x or 6.x) to Network HSM Partition (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x PCIe  HSM to a release 7.x Network HSM. You can migrate your key material using one of the following methods:

- Cloning - CPP-1859
- Backup/restore - CPP-1859
- HA - CPP-1860

## Backup and Restore

### SA5.4.7 to SA7 - PED-auth backup/restore use case

#### Preconditions

- Configure SA5.4.7 w 6.10.9 Firmware, PED-Auth/Cloning config
- Use KEYED PED
- Create a partition & challenge
- Configure SA 7.0 GA w 7.0.1 Firmware, PED-Auth/Cloning config
- Create a partition
- Install SA7 Client on Windows 2012 Server R2
- Configure client and assign partition on both SA's to the client
- You should have this
  - .246 is the SA5
  - .114 is the SA7

```
C:\Program Files\SafeNet\LunaClient>vtl list
Server: 172.20.9.246    HTL required: no
Server: 172.20.9.114    HTL required: no
```

Slot 0 is on the SA5

Slot 1 is on the SA7

```
C:\Program Files\SafeNet\LunaClient>vtl verify

The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
   0           496284016        John1
   1        152345718193
```

## Procedure

1. Run LunaCM and initialize slot 1 (the PPSO SA7 partition)

   For G5 backup/restore, you must re-use the RED key that you imprinted during partition creation the SA5, during the "par init" step on SA7

   Other keys don't matter, so re-use them

```
C:\Program Files\SafeNet\LunaClient>lunacm
LunaCM v7.0.0-262. Copyright (c) 2006-2016 SafeNet, Inc.

        Available HSMs:

        Slot Id ->              0
        HSM Label ->            John1
        HSM Serial Number ->    496284016
        HSM Model ->            LunaSA
        HSM Firmware Version -> 6.10.9
        HSM Configuration ->    Luna SA Slot (PED) Signing With Cloning Mode
        HSM Status ->           OK
        HSM Certificates ->     *** Test Certs ***


        Slot Id ->              1
        Label ->
        Serial Number ->        152345718193
        Model ->                LunaSA 7.0.0
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PED) Signing With Cloning Mode
        Slot Description ->     Net Token Slot


lunacm:> partition init -label JRSA7

        You are about to initialize the partition.
        All contents of the 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

lunacm:> role login -name po

        Please attend to the PED.

Command Result : No Error

lunacm:> role init -name co

        Please attend to the PED.

Command Result : No Error
```

```
lunacm:> role createchallenge -name co -challengeSecret johnny123

        Please attend to the PED.

Command Result : No Error

lunacm:>
```

2. Set slot to the source SA5 slot and verify object set

```
lunacm:> partition login

        Option -password was not supplied.  It is required.

        Enter the password: *******

        Please attend to the PED.

Command Result : No Error

lunacm:> partition contents

        The User is currently logged in.  Looking for objects in the
        User's partition.

        Object list:

        Label:         User Public ECDSA secp256k1 Key4
        Handle:        102
        Object Type:   Public Key
        Object UID:    18000008340200009c920700

        Label:         User Private RSA Key1-4096
        Handle:        67
        Object Type:   Private Key
        Object UID:    180000081b0200009c920700

        ................................................................

        Label:         User ARIA Key1
        Handle:        129
        Object Type:   Symmetric Key
        Object UID:    18000008510200009c920700


        Number of objects:  85


Command Result : No Error
```

3. There are multiple ways to perform a G5 backup. These are all documented as part of SA 5.4.7 documentation.

   a. Use LunaSH to perform the backup directly on the SA5

   b. Use SA5 client install lunacm to do the backup locally

   c. Use RBS backup server to perform the back to a remote G5

   The important part for us is getting those SA5 objects onto a G5 backup unit @ 6.0.8 firmware

   So, connect G5 backup device to your windows server.

   Slot list should now look like this:

```
lunacm:> slot list

        Slot Id ->              0
        HSM Label ->            John1
        HSM Serial Number ->    496284016
        HSM Model ->            LunaSA
        HSM Firmware Version -> 6.10.9
        HSM Configuration ->    Luna SA Slot (PED) Signing With Cloning Mode
        HSM Status ->           OK
        HSM Certificates ->     *** Test Certs ***


        Slot Id ->              1
        Label ->                JRSA7
        Serial Number ->        152345718193
        Model ->                LunaSA 7.0.0
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PED) Signing With Cloning Mode
        Slot Description ->     Net Token Slot


        Slot Id ->              2
        HSM Label ->            JRBackup
        HSM Serial Number ->    475292
        HSM Model ->            G5Backup
        HSM Firmware Version -> 6.0.8
        HSM Configuration ->    Luna G5 (PED) Backup Device
        HSM Status ->           OK
        HSM Certificates ->     *** Test Certs ***
```

4. Now, backup the SA5 partition contents to G5 backup device. You must reuse the same RED key you used to create the SA5 and SA7 partitions! This will preserve the cloning domain across all 3 devices.

```
lunacm:> slot set -slot 0

        Current Slot Id:    0     (Luna SA Slot 6.10.9 (PED) Signing With Cloning Mode)

Command Result : No Error

lunacm:> partition login

        Option -password was not supplied.  It is required.

        Enter the password: *******

        Please attend to the PED.

Command Result : No Error

lunacm:> partition archive backup -slot 2 -partition SA5Backup

        Logging in as the SO on slot 2.

        Please attend to the PED.

        Creating partition SA5Backup on slot 2.

        Please attend to the PED.

        Logging into the container SA5Backup on slot 2 as the user.
        Please attend to the PED.

        Creating Domain for the partition SA5Backup on slot 2.

        Please attend to the PED.

        Verifying that all objects can be backed up...

        85 objects will be backed up.

        Backing up objects...

        Cloned object 102 to partition SA5Backup (new handle 11).

        Cloned object 67 to partition SA5Backup (new handle 12).

        ................................................................

        Cloned object 129 to partition SA5Backup (new handle 120).

        Backup Complete.

        85 objects have been backed up to partition SA5Backup on slot 2.

Command Result : No Error
```

Verify all objects backup successfully as above.

5. Set slot to the SA7 partition, login the CO, and restore from G5 backup.

```
lunacm:> role login -name co

        enter password: *********

        Please attend to the PED.

Command Result : No Error

lunacm:> partition archive restore -slot 2 -partition SA5Backup

        Logging in to partition SA5Backup on slot 2 as the user.

        Please attend to the PED.

        Verifying that all objects can be restored...

        85 objects will be restored.

        Restoring objects...
        Cloned object 11 from partition SA5Backup (new handle 55).
        Cloned object 12 from partition SA5Backup (new handle 54).
        ................................................................
        Cloned object 120 from partition SA5Backup (new handle 163).

        Restore Complete.

        85 objects have been restored from partition SA5Backup on slot 2.

Command Result : No Error
```

6. Verify the partition contents on the SA7:

```
lunacm:> partition contents

        The 'Crypto Officer' is currently logged in.  Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          User ARIA Key1
        Handle:         163
        Object Type:    Symmetric Key
        Object UID:     18000008510200009c920700

        Label:          User Private RSA Key5-4096
        Handle:         159
        Object Type:    Private Key
        Object UID:     18000008230200009c920700

        ................................................................

        Label:          User Public ECDSA secp256k1 Key4
        Handle:         50
        Object Type:    Public Key
        Object UID:     18000008340200009c920700

        Number of objects:  85

Command Result : No Error
```

Keys have been restored from G5 Backup device to SA7 partition, and verified to be unchanged from the source SA5.

# Cloning

## SA 5.4.7 to SA 7 - PED-auth cloning use case

### Preconditions

- Partition to be cloned on SA 5.4.7 - must have red key from partition creation to ensure same cloning domain
- Security policy must allow cloning of private/secret keys - FIPS?
- SA7 configured and partition created
- SA7 client installed
- Source/destination partitions assigned to the client
- Verify connection to both SA's
- Verify that source/destination slots are visible

### Procedure

1. Run LunaCM and initialize the PPSO SA7 partition using the same RED key from SA5 partition creation.

```
lunacm:> partition init -label JRSA7

        You are about to initialize the partition.
        All contents of the 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

lunacm:> role login -name po

        Please attend to the PED.

Command Result : No Error

lunacm:> role init -name co

        Please attend to the PED.

Command Result : No Error

lunacm:> role createchallenge -name co -challengeSecret johnny123

        Please attend to the PED.

Command Result : No Error
```

2. Set slot to source SA5 slot and verify object set.

```
lunacm:> partition login

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

        Please attend to the PED.

Command Result : No Error

lunacm:> partition contents

        The User is currently logged in. Looking for objects in the User's partition.

        Object list:

        Label: User Public ECDSA secp256k1 Key4
        Handle: 102
        Object Type: Public Key
        Object UID: 18000008340200009c920700

        Label: User Private RSA Key1-4096
        Handle: 67
        Object Type: Private Key
        Object UID: 180000081b0200009c920700

        Label: User AES Key5
        Handle: 128
        Object Type: Symmetric Key
        Object UID: 18000008500200009c920700
....................................
        Number of objects: 85

Command Result : No Error
```

3. Clone the objects to destination SA7 slot.

```
lunacm:> partition clone -objects 0 -slot 1

        Option -password was not supplied. It is required.
        Enter the password for the target slot: *********

        Verifying that the specified objects can be cloned.

        All objects can be cloned.

        Logging in to target slot 1

        Please attend to the PED.

        Checking if objects already exist on target slot 1.

        Cloning the objects.
        Handle 102 on slot 0 is now handle 50 on slot 1
        Handle 67 on slot 0 is now handle 54 on slot 1
        Handle 128 on slot 0 is now handle 56 on slot 1
        .................................................
        Handle 129 on slot 0 is now handle 163 on slot 1

Command Result : No Error
```

4. Verify all objects have cloned successfully.

```
lunacm:> slot set -slot 1

        Current Slot Id: 1 (Luna User Slot 7.0.1 (PED) Signing With Cloning Mode)

Command Result : No Error

lunacm:> role login -name co -p johnny123

        Please attend to the PED.

Command Result : No Error

lunacm:> partition contents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label: User ARIA Key1
        Handle: 163
        Object Type: Symmetric Key
        Object UID: 18000008510200009c920700

        Label: User Private RSA Key5-4096
        Handle: 159
        Object Type: Private Key
        Object UID: 18000008230200009c920700

        Label: User DES3 Key1
        Handle: 158
        Object Type: Symmetric Key
        Object UID: 18000008470200009c920700
        ..........................................

        Number of objects: 85

Command Result : No Error
```

## SA5 to SA7 - Password-auth cloning use case

1. Ensure both the source and the target slots are visible to the client

```
lunacm:>slot list

        Slot Id ->              0
        Label ->                7sa250_pwd_p1
        Serial Number ->        154448178511
        Model ->                LunaSA 7.0.0
        Firmware Version ->     7.0.1
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     Net Token Slot

        Slot Id ->              1
        HSM Label ->            Cryptoki User
        HSM Serial Number ->    496284010
        HSM Model ->            LunaSA
        HSM Firmware Version -> 6.10.9
        HSM Configuration ->    Luna SA Slot (PW) Signing With Cloning Mode
        HSM Status ->           OK
        HSM Certificates ->     *** Test Certs ***


        Current Slot Id: 1

Command Result : No Error
```

2. Show info for the source partition - see that there is data stored

```
lunacm:>partition showinfo

        HSM Serial Number -> 496284010
        HSM Status -> OK
        HSM Certificates ->     *** Test Certs ***
        Token Flags ->
                 CKF_RNG
                 CKF_LOGIN_REQUIRED
                 CKF_USER_PIN_INITIALIZED
                 CKF_RESTORE_KEY_NOT_NEEDED
                 CKF_TOKEN_INITIALIZED
        RPV Initialized -> Not Available / Not Supported
        Slot Id -> 1
        Session State -> CKS_RW_USER_FUNCTIONS

        User Status-> Logged In

        Crypto Officer Failed Logins-> 0
        Crypto User Failed Logins->    0
        User Flags ->
                CONTAINER_KCV_CREATED
        User OUID: 14000008e70000009c920700

        User Storage:
                Total Storage Space:  2094996
                Used Storage Space:   41340
                Free Storage Space:   2053656
                Object Count:         85

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

        License Count -> 4
                1. 0009-031 Test Cert - K6 Base Configuration
                1. 620127-000 Elliptic curve cryptography
                1. 620114-000 Key backup via cloning protocol
                1. 0009-042 Test Cert - Performance Level 15

Command Result : No Error
```

3. Clone the objects from the source to the destination partition

```
lunacm:>partition clone -objects 0 -slot 0 -password userpin -force

        Verifying that the specified objects can be cloned.

        All objects can be cloned.

        Logging in to target slot 0

        Checking if objects already exist on target slot 0.

        Cloning the objects.
                Handle 15 on slot 1 is now handle 58 on slot 0
                Handle 16 on slot 1 is now handle 59 on slot
.................................................................
                Handle 124 on slot 1 is now handle 167 on slot 0

Command Result : No Error
```

# Cloning Using an HA Group

## SA 5.4.7 to SA 7 - HA group synchronization use case

### Preconditions

- SA7 must be initialized into the same cloning domain as the SA5. The red key created during SA5 initialization is required for this purpose (Actually done in Step 1).
-
-

### Procedure

1. Run LunaCM and initialize the PPSO SA7 partition.

   For HA Synchronization, you must re-use the RED key that you imprinted during the SA5 partition creation, during the "par init" step on SA7, and you must also use the same challenge as the SA5 partition - in this case "userpin".

```
lunacm:> partition init -label JRSA7
You are about to initialize the partition.
```

```
All contents of the 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

lunacm:> role login -name po
Please attend to the PED.
Command Result : No Error

lunacm:> role init -name co
Please attend to the PED.
Command Result : No Error

lunacm:> role createchallenge -name co -challengeSecret userpin
Please attend to the PED.
Command Result : No Error
```

2. Set the active slot to the source SA5 slot and verify object set.

```
lunacm:> partition login
Option -password was not supplied. It is required.
Enter the password: *******
Please attend to the PED.
Command Result : No Error

lunacm:> partition contents
The User is currently logged in. Looking for objects in the
User's partition.
Object list:
Label: User Public ECDSA secp256k1 Key4
Handle: 102
Object Type: Public Key
Object UID: 18000008340200009c920700
Label: User Private RSA Key1-4096
Handle: 67
Object Type: Private Key
Object UID: 180000081b0200009c920700
.......................................
Object Type: Symmetric Key
Object UID: 18000008510200009c920700
Number of objects: 85
Command Result : No Error
```

3. Using LunaCM, create an HA group of the SA5 slot and the SA7 slot.

> **Note:** HA requires that all members have an activation policy set. Consult the SA5 and SA7 documentation for details.

   a. On SA5, log in as SO and set policy 22 via LunaSH:

```
[5sa246] lunash:>partition changepolicy -partition John1 -policy 22 -value 1
'partition changePolicy' successful.
Policy "Allow activation" is now set to: 1
Command Result : 0 (Success)
```

   b. On SA7, log in as PSO, and set the activation policy in LunaCM from the client machine:

```
lunacm:> slot set -slot 1
Current Slot Id: 1 (Luna User Slot 7.0.1 (PED) Signing With Cloning Mode)
```

```
Command Result : No Error

lunacm:> role login -name po
Please attend to the PED.
Command Result : No Error

lunacm:> partition changepolicy -p 22 -v 1
Command Result : No Error
```

c. Create the HA group, pointing to the SA5 partition as the primary partition. Select the "copy" option to preserve objects!

```
lunacm:> ha creategroup -label JRHA -slot 0 -p userpin
Warning: There are objects currently on the new member.
Do you wish to propagate these objects within the HA
group, or remove them?
Type 'copy' to keep and propagate the existing
objects, 'remove' to remove them before continuing,
or 'quit' to stop adding this new group member.
> copy
New group with label "JRHA" created with group number 1496284016.
Group configuration is:
HA Group Label: JRHA
HA Group Number: 1496284016
HA Group Slot ID: Not Available
Synchronization: enabled
Group Members: 496284016
Needs sync: no
Standby Members: <none>
Slot # Member S/N Member Label Status
====== ========== ============ ======
0 496284016 John1 alive
Command Result : No Error
```

d. Add the SA7 slot to the HA group. Repeat this step to add multiple SA7 HSMs to the group.

```
lunacm:> ha addmember -group JRHA -slot 1 -p userpin
Member 152345718193 successfully added to group JRHA. New group
configuration is:
HA Group Label: JRHA
HA Group Number: 1496284016
HA Group Slot ID: Not Available
Synchronization: enabled
Group Members: 496284016, 152345718193
Needs sync: yes
Standby Members: <none>
Slot # Member S/N Member Label Status
====== ========== ============ ======
0 496284016 John1 alive
1 152345718193 JRSA7 alive
Please use the command "ha synchronize" when you are ready
to replicate data between all members of the HA group.
(If you have additional members to add, you may wish to wait
until you have added them before synchronizing to save time by
avoiding multiple synchronizations.)
Command Result : No Error
```

4. Synchronize the group to clone the objects to the SA7 member(s).

```
lunacm:> ha synchronize -group JRHA -p userpin
Synchronization completed.
Command Result : No Error
```

5. Check synchronization status of the group.

```
lunacm:> ha listgroups
If you would like to see synchronization data for group JRHA,
please enter the password for the group members. Sync info
not available in HA Only mode.
Enter the password: *******
HA auto recovery: disabled
HA recovery mode: passive
Maximum auto recovery retry: 0
Auto recovery poll interval: 60 seconds
HA logging: disabled
Only Show HA Slots: no
HA Group Label: JRHA
HA Group Number: 1496284016
HA Group Slot ID: Not Available
Synchronization: enabled
Group Members: 496284016, 152345718193
Needs sync: no
Standby Members: <none>
Slot # Member S/N Member Label Status
====== ========== ============ ======
0 496284016 John1 alive
1 152345718193 JRSA7 alive
Command Result : No Error
```

Notice the entry "Needs sync: no". To be doubly sure, log in to the SA7 slot and check the partition contents:

```
lunacm:> slot set -s 1
Current Slot Id: 1 (Luna User Slot 7.0.1 (PED) Signing With Cloning Mode)
Command Result : No Error

lunacm:> role login -name co
enter password: *******
Command Result : No Error

lunacm:> par con
The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.
Object list:
Label: User ARIA Key1
Handle: 163
Object Type: Symmetric Key
Object UID: 18000008510200009c920700
Label: User Private RSA Key5-4096
Handle: 159
Object Type: Private Key
Object UID: 18000008230200009c920700
Label: User DES3 Key1
Handle: 158
.......................................
Object Type: Public Key
Object UID: 18000008340200009c920700
Number of objects: 85
Command Result : No Error
```

# 2 PCIe HSM (5.x or 6.x) to Network HSM Partition (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x PCIe HSM to a release 7.x Network HSM. You can migrate your key material using one of the following methods:

Cloning - CPP-422

Backup/restore - CPP-422

## Backup and Restore

## Cloning

# 3

# PCIe or USB HSM (5.x or 6.x) to PCIe HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x PCIe or USB HSM to a release 7.x PCIe HSM. You can migrate your key material using one of the following methods:

- Cloning - CPP_424 (USB,PCI), CPP-420 (PCI)
- Backup/restore - CPP_424 (USB,PCI), CPP-420 (PCI)

  no backup/restore for G5 1.2 and 1.3
- HA - CPP-424 (PCIe), CPP-420 (PCI)

## Backup and Restore

## Cloning

### G5 1.3 with FW 6.2.1 CentOS 5 64bits to K7 7.0.1 CentOS 7 64bits - PW-Auth cloning use case

#### Preconditions

- Partition to be cloned on CentOS client with K7 7.0.1 installed and G5 option enabled?
- G5 USB connected to client and LunaCM can see both K7 and G5.
-

#### Procedure

1. Create a new K7 Partition
   a. Set slot to an existing K7 partition.

   ```
   lunacm:>s s s 205
   Current Slot Id:  205     (Luna Admin Slot 7.0.1 (PW) Signing With Cloning Mode)
   Command Result : No Error
   lunacm:>
   ```

   b. Set role to SO.

   ```
   lunacm:>role login -n so
   enter password: *******
   ```

```
Command Result : No Error
lunacm:>
```

c. Create partition.

```
lunacm:> lunacm:>par crp
Command Result : No Error
lunacm:>
```

d. Confirm that new partition was created.

```
lunacm:>s l
Slot Id ->              0
HSM Label ->            no label
HSM Serial Number ->    150666
HSM Model ->            K6Base
HSM Firmware Version -> 6.20.0
HSM Configuration ->    Luna PCI (PED) Signing Mode
HSM Status ->           Transport Mode, Zeroized
HSM Certificates ->     *** Test Certs ***

Slot Id ->              1
HSM Label ->            seghu
HSM Serial Number ->    7001968
HSM Model ->            G5Base
HSM Firmware Version -> 6.2.1
HSM Configuration ->    Luna G5 (PW) Signing With Cloning Mode
HSM Status ->           OK
HSM Certificates ->     *** Test Certs ***

Slot Id ->              104
Label ->
Serial Number ->        67841
Model ->                Luna K7
Firmware Version ->     7.0.1
Configuration ->        Luna HSM Admin Partition (PW) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PW)
HSM Status ->           L3 Device, Zeroized
HSM Certificates ->     *** Test Certs ***

Slot Id ->              105
Label ->                k7par1
Serial Number ->        158073350953
Model ->                Luna K7
Firmware Version ->     7.0.1
Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              106
Label ->
Serial Number ->        158073350954
Model ->                Luna K7
Firmware Version ->     7.0.1
Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              107
Label ->
Serial Number ->        158073350955
Model ->                Luna K7
Firmware Version ->     7.0.1
```

```
Configuration ->         Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->      User Token Slot

Slot Id ->               205
Label ->                 K7892
Serial Number ->         67892
Model ->                 Luna K7
Firmware Version ->      7.0.1
Configuration ->         Luna HSM Admin Partition (PW) Signing With Cloning Mode
Slot Description ->      Admin Token Slot
HSM Configuration ->     Luna HSM Admin Partition (PW)
HSM Status ->            L3 Device, Card removal
HSM Certificates ->      *** Test Certs ***

Current Slot Id: 205
Command Result : No Error
Lunacm:>
```

**Note:** New partition is in slot 107.

2. Initialize the new K7 partition with the same domain as the G5 partition.

```
lunacm:>s s s 107
Current Slot Id:  107     (Luna User Slot 7.0.1 (PW) Signing With Cloning Mode)
Command Result : No Error

lunacm:>par init -l migrationpartition
You are about to initialize the partition.
All contents of the partition will be destroyed.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now ->proceed
Enter password for Partition SO: *******
Re-enter password for Partition SO: *******
Option -domain was not specified.  It is required.
Enter the domain name: *******
Re-enter the domain name: *******
Command Result : No Error
```

3. Initialize the CO role for the new K7 partition.

```
lunacm:>role login -n po
enter password: *******
Command Result : No Error

lunacm:>role init -n co
enter new password: *******
re-enter new password: *******
Command Result : No Error

lunacm:>
```

4.

# Cloning Using an HA Group

# 4
# Network HSM Partiton (5.x or 6.x) to PCIe HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x Network HSM partition to a release 7.x PCIe HSM. You can migrate your key material using one of the following methods:

- Cloning
- Backup/restore - CPP-421

## Backup and Restore

## Cloning