Luna HSM Create Partition

Document Information	
Namn	Luna HSM Create Partition
Version	1.1
Editor	Leif Johansson
Date	2014-05-14
Changes	1.1 – Permit auto activation

Purpose and scope

This procedure ensures that a partition is created in the Luna HSM platform.

Governing policies

This procedure is governed by the following policies:

- SUNET Key Management Policy (SUNET KMP)
- SUNET Asymmetric HSM Service Key Management Practice Statement (SUNET HSM KMPS)

Roles

Number of Persons	Role Name	Responsibilities
1	KCO	Note taking. Driving the process
2	SO	Authenticate to the HSM and the cloning domain

Procedure Steps

Role	Description
KCO	**Preparation** 1. Login to the HSM appliance 2. Connect the PED (local or remote)
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
Both SO	**SO keyset safe extract** 1. SOs open their safe deposit boxes 2. Extract the SO keyset tamper evident bags 3. Compare the tamper evident bag seals with the records in the log 4. Record the incoming tamper evident bag seals below

Completed (yes/no)	Notes
	<table><tr><td>**SO Name**</td><td>**Tamper Bag Serial**</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>

Time &Date	Signature/Initial

Role	Description
KCO + both SOs	**Authenticate to the HSM** At the HSM appliance prompt type: # hsm login Both SOs in turn connect their blue PED keys to the PED to complete the authentication.

Completed (yes/no)	Notes

Time &Date	Signature/Initial

Role	Description
KCO + both SOs in case the main cloning domain will be used	**Create the Partition** At the HSM appliance prompt type: # partition create –partition <partition name> The PED will prompt for creating a black PED keyset for the partition owner. The Key Management Practice statement (KMPS) of the application that will use the partition governs the choices (pins, M-by-N, backup keysets etc) made in this step. **During this process the PED will prompt for a cloning domain keyset. Normally the main SO domain keyset should be used or backups of the partition can't be done by the SUNET KMF. To re-use the main HSM KMF cloning domain, both the SOs should connect their primary red PED keys to the PED when prompted.** When the process finishes the HSM appliance shell returns a prompt indicating success and the PED displays a partition password: 4 groups of 4 characters separated by dashes ('-'). Make a careful record of this password below. Optionally and conditioned on the KMPS of the application owning the partition the partition may be activated and the partition policy may be changed to auto-activation at this time.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
Both SO	**SO keyset safe deposit**

1. SOs deposit their PED key chains in separate tamper evident bags.
2. Make a record of the SO outgoing tamper evident seal serials below

SO Name	Tamper Bag Serial

3. The SOs deposits the tamper evident bags in their individual deposit boxes.

Completed (yes/no)	Notes

Time &Date	Signature/Initial

Role	Description
KCO	**Finish up**

1. At the HSM appliance prompt type:

   # hsm logout

2. Close the HSM appliance ssh session
3. Disconnect the PED and store all relevant equipment in the safe
4. Include this document in the log
5. Close the safe

Completed (yes/no)	Notes

Time &Date	Signature/Initial