SUNET KMF Procedure

Luna HSM Initialization

Document Information	
Namn	Luna HSM Initialization
Version	1.0
Editor	Leif Johansson
Date	2014-05-13

Purpose and scope

This procedure ensures that a set of Security Officers (SO) are established and that an HSM acting as the first member of a cluster is initialized with a new set of HSM admin keys. A new cloning domain is also created.

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
5	SO	Take ownership of a set of HSM/Domain PED keys
1	KCO	Note-taking and record keeping. Operating the Luna HSM appliance

Summary

Each SO will initialize a primary and a secondary PED keyset. Each keyset consists of a blue HSM PED key and a red Cloning Domain PED key. The actual initialization process must be completed without interruptions so it is necessary to have all materials prepared before starting.

During the initialization process the PED will prompt for actions. Refer to the Luna SA5 documentation for details about what to expect.

Since PED keysets are stored in tamper-evident bags in personal safe storage boxes between use, this process does not use the PIN feature of the Luna platform. All PINs are set to <empty>. The process uses a 2-by-5 (M-by-N) split of the HSM and Cloning Domain keysets. This means that all following SO operations can proceed with only 2 SOs present as described in the SUNET HSM KMPS.

The blue PED keys authenticate access to the HSM itself. The red PED keys authenticates access to and encrypts the keys stored on the HSM. In the SUNET KMPS the SO is responsible for both PED keysets. The Luna SA5 platform requires these keysets to be kept physically distinct.

Procedure Steps

Role	Description
KCO	Prepare materials • Unpack and label 5+5 blue PED keys (HSM keyset+backup) • Unpack and label 5+5 red PED keys (Domain keyset+backup) • Unpack 5+5 tamper-evident bags • Assign each SO a personal safe storage box & key
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
SO	Take ownership of PED keysets Each SO picks a set of 2+2 PED keys – one primary and one backup. Each pair of a blue and a red PED key is placed on a keychain which is labeled “Primary” and “Backup”.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
KCO	HSM Initialization Login to HSM appliance. Connect a PED terminal to the PED port (or use a remote PED). Issue the following command at the HSM appliance prompt: # hsm init –label <name of hsm> Follow the directions in the PED display. Use the following answers for the Blue and Red PED keyset prompts: **Reuse existing keyset: No** **M-value: 2** **N-value: 5** **PED PIN: <empty> (no PED pins are used)** When prompted at the PED, insert the blue PED key of the Primary keychain of each SO. After this is done choose to duplicate the keyset and insert the blue PED key of the Backup keychain of each SO. At this point proceed to creating the cloning domain. The cloning domain is created using the same process: first insert each primary Red SO key and then, when duplicating the cloning keyset, insert each backup Red SO key. After completing this the HSM terminal prompt should indicate success.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
SO+KCO	PED Keyset Safe Deposit Each SO deposits the primary and backup in separate tamper-evident bags. Each bag is deposited in the SO personal safe storage. Record the serial numbers of each bag below:
Completed (yes/no)	**Notes**
	SO tamper-evident bag serials SO Name | Primary keyset | Backup keyset | | | | | | | | | | | | | | | | | | | |
Time &Date	**Signature/Initial**

Role	Description
KCO	Finish up Ensure all safe deposit boxes are closed. Close safe, logout from HSM appliance.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**