SUNET

SUNET KMF Procedure

Luna HSM Remote PED Keyset Creation

Document Information	
Namn	Process name
Version	1.0
Editor	Leif Johansson
Date	2014-05-15

Purpose and scope

This procedure ensures that a remote PED key 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)

Security Constraints

The orange remote PED key is used to authenticate the PED terminal to the HSM when it is operating in remote mode (i.e. when not connected directly to the HSM front panel). Access to a remote PED key is comparable to having access to an SSH key for authenticating to the HSM and will be treated in the same way as any other server authentication token. The orange PED keys are assigned to KCOs and shall be treated as a sensitive access credentials.

Roles

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

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**

<table>
<tr><th>Role</th><th>Description</th></tr>
<tr><td>Both SO</td><td>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</td></tr>
<tr><th>Completed (yes/no)</th><th>Notes</th></tr>
<tr><td></td><td><table><tr><th>SO Name</th><th>Tamper Bag Serial</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><th>Time &Date</th><th>Signature/Initial</th></tr>
<tr><td></td><td></td></tr>
<tr><th>Role</th><th>Description</th></tr>
<tr><td>KCO + both SOs</td><td>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.</td></tr>
<tr><th>Completed (yes/no)</th><th>Notes</th></tr>
<tr><td></td><td></td></tr>
<tr><th>Time &Date</th><th>Signature/Initial</th></tr>
<tr><td></td><td></td></tr>
</table>

Role	Description
KCO + both SOs in case the main cloning domain will be used	Initialize remote PED keyset At the HSM appliance prompt type: # hsm ped vector init The PED will prompt for creating an orange remote PED keyset. Create enough remote PED keys to assign to all KCOs + at least 2 duplicates. Unassigned remote PED keys are kept in a tamper evident bag until assigned to a KCO via the remote PED key assignment form. Each time a PED key is assigned to a KCO a new bag is assigned and the incoming and outgoing bag tamper seals are recorded in the PED key assignment form.
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**

Role	Description
SO	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** | **Tamper Bag Serial** | | | |
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**