Document Information

Luna HSM Shipping

Purpose and scope

This procedure ensures that a Luna HSM is enabled for safe transport.

Governing policies

This procedure is governed by the following policies:

- SUNET Key Management Policy (SUNET KMP)
- SUNET Asymmetric HSM KMPS

Roles

Number of Persons	Role Name	Responsibilities
1	SO	SRK resplit token holder
1	SO	Record keeping and oversight

Summary

The following process prepares a Luna HSM for shipping to a remote location/site by enabling “SRK Resplit Mode” and “Secure Transport Mode”.

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>
</table>

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
SO	Enable SRK resplit token Before proceeding allocate 2 SRK resplit tokens - either new or already labeled with the purple tags – one for each SO present. In the Luna HSM shell: **# hsm srk enable** In the PED (remote or local) answer the following prompts (user input in bold): M value (1-16): **2** N value (M-16): **2** Insert the two SRK resplit keys in turn and elect to overwrite the SRK key. **NOTE That if multiple HSMs are shipped at the same time, multiple SRK keysets must be allocated and kept separate.** After this step completes, the PED should say “STM Enabled”. Verify by doing the following: **# hsm srk show** Secure Recovery State flags: ==================================== External split enabled: yes **SRK** resplit required: no Hardware tampered: no Transport mode: no Command Result : 0 (Success)
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
SO	Enable Transport Mode Issue the following command at the prompt: **# hsm srk transportMode enter** In the PED (remote or local) insert the SRK keys when prompted. Make a note of the verification string displayed in the PED below. The PED should display the message “SRK was zeroized” if the procedure was successful. Verify by doing the following: **# hsm srk show** Secure Recovery State flags: ================================= External split enabled: yes **SRK** resplit required: no Hardware tampered: no Transport mode: yes The HSM is now ready for shipping.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

<table>
<tr><td><b>Role</b></td><td><b>Description</b></td></tr>
<tr><td>SO</td><td>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:</td></tr>
<tr><td><b>Completed (yes/no)</b></td><td><b>Notes</b></td></tr>
<tr><td></td><td>SO tamper-evident bag serials
<table>
<tr><td><b>SO Name</b></td><td><b>Tamper Bag Serial</b></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table></td></tr>
<tr><td><b>Time &Date</b></td><td><b>Signature/Initial</b></td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Role</b></td><td><b>Description</b></td></tr>
<tr><td>KCO</td><td>Finish up
Ensure all safe deposit boxes are closed. Close safe, logout from HSM appliance.</td></tr>
<tr><td><b>Completed (yes/no)</b></td><td><b>Notes</b></td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Time &Date</b></td><td><b>Signature/Initial</b></td></tr>
<tr><td></td><td></td></tr>
</table>