SUNET

SUNET KMF Procedure

YubiHSM KCO Enrollment

Document Information

Namn	YubiHSM KCO Enrollment
Version	1.1
Editor	Leif Johansson
Date	2014-05-23

1. Purpose and scope

This procedure ensures that a new KCO is identified and credentialed for the YubiHSM KMPS

2. Governing policies

This procedure is governed by the following policies:

- SUNET Key Management Policy (SUNET KMP)
- SUNET Symmetric (YubiHSM) Key Management Policy

3. Roles

Number of Persons	Role Name	Responsibilities
1	SO	Note-taking and oversight
1	KCO	Decrypt full disk encryption on programming station

4. Procedure Steps

Role	Description
SO	Safe Extraction The SO opens the safe an extracts the RED ZONE KCO programming station together with a random number generator (USB key) and an unused YubiKey for each KCO to be enrolled
Completed (yes/no)	**Notes**
	The following KCOs are enrolled/deprovisioned:
Time &Date	**Signature/Initial**

Name	YubiKey Serial	Enrolled/Deprovision

Role	Description
KCO	Boot the programming station An existing KCO is needed to unlock full disk encryption on the programming station. The shell login for user root is taped to the laptop. Login as root.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
KCO	Enable entropy device (araneus) 1. Connect the araneus device 2. Start the entropy daemon in the background # araneus_rngd &
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description

	KCO Enrollment
	Each YubiHSM KCO has a YubiKey in static mode which in combination with a personal password (salt) is used to enable full disk encryption on the PS. The YubiKey must be inserted into a USB port.
	To configure a YubiKey in static mode (should be done on PS, using attached HW RNG):
	`# ykpersonalize -2`
	The -2 selects virtual slot #2 in the YubiKey which has the correct settings for a static key by default. At the prompt for AES key press ‘Enter’ and then at the “Commit ?”-prompt press ‘y’.
	To add a new KCO to the LUKS header (full disk encryption) of the PS:
	Find unused slot in LUKS header (look for Key Slot X: DISABLED)
	`# cryptsetup luksDump /dev/sda2`
	Add a new KCO key to Key Slot X (this requires cooperation of one existing KCO, and the one to be added): Before running this command select and memorize a short PIN or password which will be combined with the YubiKey static secret.
	`# cryptsetup luksAddKey --key-slot X /dev/sda2`
	The first password prompt is for any of the currently active KCOs keys. Follow the same process as below (PIN followed by 3-5s press on the YubiKey).
	At the password-prompt, type your PIN followed by a press on the YubiKey for 3-5 seconds to select the second virtual slot in the YubiKey which carries the static secret.
	Verify that LUKS Key Slot X is now ENABLED:
	`# cryptsetup luksDump /dev/sda2`
	To remove a key, enter the key to the following command:
	`# cryptsetup luksRemoveKey /dev/sda2`
	As long as the key is known, it can be removed without knowing the Key Slot number. Removing a key will also require authentication from a currently active KCO.

Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	**Description**
KCO	Test the new KCO keys Reboot the programming station once for each new KCO key and verify that the newly generated YubiKeys can unlock the programming station.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	**Description**
KCO+SO	Shutdown programming station Shutdown& turn of the programming and deposit the KCO YubiKeys (on separate key-chains) in the respective deposit boxes of the KCOs. Close all depositboxes and close the safe.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**