SUNET

SUNET KMF Procedure

YubiHSM HMAC Key Generation

Document Information	
Namn	YubiHSM HMAC Key Generation
Version	1.0
Editor	Leif Johansson
Date	2014-11-19

Purpose and scope

This procedure ensures that a new high-quality HMAC key is generated and stored on a YubiHSM.

Governing policies

This procedure is governed by the following policies:

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

Roles

Number of Persons	Role Name	Responsibilities
1	SO	Monitor and document process
1	KCO	Operates Programming Station (PS). Unlocks YubiHSM using YubiHSM Master Key

Key Naming

Keys generated in this process are assigned key handles. In order to simplify application integration key handles are named using the current date combined with a letter indicating key usage.

The program `vccs-configure-hsms' will suggest key handles using this scheme: Assuming the date is 2014-02-21, the regular password credential HMAC key is called 0x140221aa and the OATH credential HMAC key is called 0x140221da. If a second key needs to be created the same day, it should be called 0x<date>ab or 0x<date>db, where <date> is replaced by the current date in the format yymmdd. This date is used to expire the key handle.

Procedure Steps

The process consists of several steps. In general a set of YubiHSMs are created with the same set of keys. The keys are stored in a database on the PS. Before any of the key generation steps are started the Preparation Step must be completed. Both procedures start with the Preparation step and ends with the End Procedure step. **Note that it may be more efficient to interleave the steps below for each YubiHSM used instead of switching YubiHSMs.**

The steps for creating a YubiHSM for password credentials is as follows:

1. (Optional) YubiHSM initialization (once for all YubiHSMs used)
2. Create Primary Password Credentials Key in PS database
3. Install Primary Password Credentials Key (from step 3) on a sufficient number of YubiHSMs

The steps for creating a YubiHSM for OATH credentials is as follows:

1. (Optional) YubiHSM initialization (once for all YubiHSMs used)
2. Create Primary OATH Credentials Key in PS database
3. Install Primary OATH Credentials Key (from step 3) as ORIGINATOR on one YubiHSM
4. Install Primary OATH Credentials Key (from step 3) as VALIDATOR on a sufficient number of YubiHSM

Role	Description
SO+KCO	Preparation Retrieve the KCO FDE (full disk encryption) key from KCO personal safe storage and recall the salt password to memory. The FDE key is a yubikey configured as a static password and is stored in the KCO personal safe storage. Retrieve PS from BLACK zone safe and connect the PS to power. Make sure to face the screen away from any cameras, windows or reflective surfaces to avoid “shoulder-surfing” information displayed on the screen. Power on the PS (KCO) and use the KCO yubikey to unlock Full Disk Encryption during the boot process. Finally the KCO logs in as “root” (password can be found on the bottom of the PS) to complete the step.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
KCO	YubiHSM Bootstrap/Initialization **This is an OPTIONAL step performed as/if needed.** To bootstrap a brand new HSM (or one whose configuration has been reset using the 'zap' CLI command) use the following steps: Put the YubiHSM in programming mode by pressing the reset button (with an “ejecttrode”) at the same time as the YubiHSM is inserted in the USB port. **# ./vccs-configure-hsms --init** During initialization the HSM asks for a Master Key (MSK). Choose the key serial number as displayed on the screen.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description

KCO	Create Primary HSM Password Credentials Key
	
	Insert the YubiHSM while pressing the button underneath the hole to put the key into programming mode.
	
	# ./vccs-configure-hsms --gen_key
	
	`Insert a YubiHSM and press enter *ENTER*`
	`INFO Detected YubiHSM with id : xxx`
	`Enter new key handle (press enter for '<date>aa') :`
	`INFO New key '<date>aa' added to key database.`

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

Role	Description

KCO	Create Primary OATH Credentials Key
	
	Insert the YubiHSM while pressing the button underneath the hole to put the key into programming mode.
	
	# ./vccs-configure-hsms --gen_key --key_usage oath
	
	`Insert a YubiHSM and press enter *ENTER*`
	`INFO Detected YubiHSM with id : xxx`
	`Enter new key handle (press enter for '<date>da') :`
	`INFO New key '<date>da' added to key database.`

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

Role	Description
KCO	Install Primary Password Credentials Key Be prepared to enter the Master Key to unlock the configuration if prompted during this step. Repeat this process for all active keys of the same type in the database. Put the YubiHSM in programming mode by pressing the reset button (with an “ejecttrode”) at the same time as the YubiHSM is inserted in the USB port. **# ./vccs-configure-hsms --max_key_age 1095 --install_keys <date>aa** Insert a YubiHSM and press enter ***ENTER*** INFO Detected YubiHSM with id : xxx INFO INFO Keys now in HSM : INFO <date>aa (age: 0 day(s), flags=0x10000, usage=unknown) Commit changes to keystore? Enter 'yes' or 'no' : yes INFO xxx Keys committed to keystore.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description
KCO	Install Primary OATH Credentials Key as VALIDATOR Be prepared to enter the Master Key (MSK) to unlock the configuration if prompted during this step. Repeat this process for all active keys of the same type in the database. **# ./vccs-configure-hsms --max_key_age 1095 --install_keys <date>da --key_usage oath** Insert a YubiHSM and press enter ***ENTER*** INFO Detected YubiHSM with id : xxx INFO INFO Keys now in HSM : INFO <date>aa (age: 0 day(s), flags=0x10000, usage=unknown) INFO <date>da (age: 0 day(s), flags=0x20000, usage=unknown) Commit changes to keystore? Enter 'yes' or 'no' : yes INFO xxx Keys committed to keystore.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	Description

KCO	Install Primary OATH Credentials Key as ORIGINATOR
	Be prepared to enter the Master Key (MSK) to unlock the configuration if prompted during this step. Repeat this process for all active keys of the same type in the database.
	# ./vccs-configure-hsms --max_key_age 1095 --install_keys <date>da --key_usage oath --originator
	`Insert a YubiHSM and press enter *ENTER*`
	`INFO Detected YubiHSM with id : xxx`
	`INFO`
	`INFO Keys now in HSM :`
	`INFO <date>da (age: 0 day(s), flags=0x2, usage=unknown)`
	`Commit changes to keystore? Enter 'yes' or 'no' : yes`
	`INFO xxx Keys committed to keystore.`

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

Role	Description
KCO	End Procedure Shutdown PS, return to SAFE. Return KCO yubikey to personal safe storage.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**