# Root DNSSEC KSK Ceremony 53-2

Friday 26 April 2024

Root Zone KSK Operator Key Management Facility
18155 Technology Drive, Culpeper, VA 22701, USA

This ceremony is executed in accordance with the DNSSEC Practice Statement for the Root Zone KSK Operator 7th Edition (2024-03-15)

## Abbreviations

| | |
|---|---|
| **AUD** | = Third Party Auditor |
| **EW** | = External Witness |
| **IW** | = Internal Witness |
| **MC** | = Master of Ceremonies |
| **RKSH** | = Recovery Key Share Holder |
| **SA** | = System Administrator |
| **SO** | = Security Officer |
| **SW** | = Staff Witness |
| **CA** | = Ceremony Administrator |
| **FD** | = Flash Drive |
| **KMF** | = Key Management Facility |
| **OP** | = Operator |
| **RKOS** | = RZ KSK Operations Security |
| **SKR** | = Signed Key Response |
| **SSC** | = Safe Security Controller |
| **TCR** | = Trusted Community Representative |
| **CO** | = Crypto Officer |
| **HSM** | = Hardware Security Module |
| **KSR** | = Key Signing Request |
| **PTI** | = Public Technical Identifiers |
| **RZM** | = Root Zone Maintainer |
| **SMK** | = Storage Master Key |
| **STM** | = Secure Transport Mode |
| **TEB** | = Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20) |

## Participants

Key Ceremony roles are described on https://www.iana.org/help/key-ceremony-roles
**Instructions:** At the end of the ceremony, participants sign IW's script. IW records time of completion.

| Title / Roles | Printed Name | Signature | Date | Time |
|---|---|---|---|---|
| CA | David Huberman / ICANN | | 2024 Apr 26 | 22:20 |
| IW | Yuko Yokoyama / ICANN | | | |
| SSC1 | Fernanda Iunes / ICANN | | | |
| SSC2 | Hope Shafer / ICANN | | | |
| MC | Matthew Larson / ICANN | | | |
| CO1 | Frederico Neves | | | |
| CO2 | Pia Gruvö | | | |
| CO3 | Ondrej Filip | | | |
| CO4 | Robert Seastrom | | | |
| CO5 | Nomsa Mwayenga | | | |
| CO6 | Hugo Salgado | | | |
| CO7 | Dileepa Lathsara | | | |
| RKSH1 | Sebastian Castro | | | |
| RKSH2 | Ondřej Surý | | | |
| RKSH3 | Kristian Ørmen | | | |
| RKSH4 | Jiankang Yao | | | |
| RKSH5 | Bevil Wooding | | | |
| RKSH6 | John Curran | | | |
| RKSH7 | Dave Lawrence | | | |
| AUD | Melanie Chen / RSM | | | |
| AUD | Grant An / RSM | Grant an | | |
| SA | Reed Quinn / ICANN | Reed | | |
| RKOS / CA Backup | Andres Pavez / PTI | | | |
| RKOS / IW Backup | Aaron Foley / PTI | | | |
| SW | Kim Davies / PTI | | | |
| EW | Ólafur Guðmundsson / CO5 West | | | |
| | Guth | | | |
| | | | | |
| | | | | |

***By signing this script, you are declaring that this document is a true and accurate record of the Root DNSSEC KSK ceremony to the best of your knowledge, and you agree that your personal data will be processed in accordance with the ICANN Privacy Policy available at https://www.icann.org/privacy/policy***

# Instructions for a Root DNSSEC KSK Ceremony

The Root DNSSEC Key Signing Key (KSK) Ceremony is a scripted meeting where individuals with specific roles generate or access the private key component of the root zone DNSSEC KSK. The process is audited by a third party firm for compliance with SOC 3 framework. The script and recordings are published online for the wider Internet community to review.

**Ceremony Guidelines:**

- The CA leads the ceremony
- Only a CA, IW, or SA can enter and escort other participants into Tier 4 (Key Ceremony Room)
- Dual Occupancy is enforced. IW with CA or SA must remain inside Tier 4 (Key Ceremony Room) if participants are present in the room
- During a ceremony a CA, IW, or SA may escort participants out of Tier 4 (Key Ceremony Room) at the CA's discretion if Tier 5 (Safe Room) is not occupied
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log located in Tier 3
- The SA begins recording with the audit cameras shortly before the ceremony begins
- Ceremony participants follow the script step by step in order to attest to the ceremony's proper performance
- The CA reads each step aloud prior to its performance
- Upon the successful completion of a step, the IW will announce and record its time of completion, and initials that step in their script
- A ceremony participant who has cause for concern or detects an issue is encouraged to interrupt the ceremony for discussion. The issue is brought to resolution before the ceremony resumes
- Questions and suggestions for improvement are welcome and can be discussed at any time or after the ceremony during the ceremony debrief

Unplanned events **(exceptions)** during the ceremony are evaluated, documented, and acted upon. It is the CA's sole responsibility to decide on proper actions after consulting with the IW. In either case, an exception is regarded as an incident, and incident handling procedures are enacted.

Key Management Facility Tiers:

- Tiers 1-3: Consist of the facility areas between the outside environment and the Key Ceremony Room
- Tier 4: Consists of the Key Ceremony Room and is subject to Dual Occupancy
- Tier 5: Consists of the Safe Room (a cage only accessible from the Key Ceremony Room) and is subject to Dual Occupancy
- Tier 6: Consists of Safe #1 (Equipment Safe) and Safe #2 (Credentials Safe)
- Tier 7: Consists of the HSMs stored in Safe #1 (Equipment Safe) and the safe deposit boxes installed in Safe #2 (Credentials Safe)

Some steps during the ceremony may require the participants to recite and/or confirm identifiers comprised of numbers and letters. When spelling identifiers, the phonetic alphabet shown below should be used:

| Character | Code Word | Pronunciation |
|---|---|---|
| **A** | Alfa | AL-FAH |
| **B** | Bravo | BRAH-VOH |
| **C** | Charlie | CHAR-LEE |
| **D** | Delta | DELL-TAH |
| **E** | Echo | ECK-OH |
| **F** | Foxtrot | FOKS-TROT |
| **G** | Golf | GOLF |
| **H** | Hotel | HOH-TEL |
| **I** | India | IN-DEE-AH |
| **J** | Juliet | JEW-LEE-ETT |
| **K** | Kilo | KEY-LOH |
| **L** | Lima | LEE-MAH |
| **M** | Mike | MIKE |
| **N** | November | NO-VEM-BER |
| **O** | Oscar | OSS-CAH |
| **P** | Papa | PAH-PAH |
| **Q** | Quebec | KEH-BECK |
| **R** | Romeo | ROW-ME-OH |
| **S** | Sierra | SEE-AIR-RAH |
| **T** | Tango | TANG-GO |
| **U** | Uniform | YOU-NEE-FORM |
| **V** | Victor | VIK-TAH |
| **W** | Whiskey | WISS-KEY |
| **X** | Xray | ECKS-RAY |
| **Y** | Yankee | YANG-KEY |
| **Z** | Zulu | ZOO-LOO |
| **1** | One | WUN |
| **2** | Two | TOO |
| **3** | Three | TREE |
| **4** | Four | FOW-ER |
| **5** | Five | FIFE |
| **6** | Six | SIX |
| **7** | Seven | SEV-EN |
| **8** | Eight | AIT |
| **9** | Nine | NIN-ER |
| **0** | Zero | ZEE-RO |

# Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

- Verify that the audit cameras are recording and the online video streaming is active
- Confirm that all of the ceremony attendees have signed in using the visitor log in Tier 3
- Review emergency evacuation procedures
- Explain the use of personal devices and the purpose of this ceremony
- Verify the time and date so that all entries into the script follow a common time source
- Explain the purpose of the ceremony along with a high-level list of tasks to be completed

The CA and IW will then escort the SSC into Tier 5 (Safe Room) to retrieve required materials from the following location:

- Safe #1 containing all equipment: HSMs, laptops, OS media, etc

## Sign into Tier 4 (Key Ceremony Room)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1.1 | CA confirms with SA that all audit cameras are recording and online video streaming is active. | Y.Y. | 14:01 |
| 1.2 | CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2. | Y.Y. | 14:02 |
| 1.3 | CA asks that any first-time ceremony participants in the room introduce themselves. | Y.Y. | 14:03 |

## Emergency Evacuation Procedures and Electronics Policy

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1.4 | CA reviews emergency evacuation procedures with onsite participants. | Y.Y. | 14:03 |
| 1.5 | CA explains the use of personal electronic devices during the ceremony. | Y.Y. | 14:03 |
| 1.6 | CA summarizes the purpose of the ceremony. | Y.Y. | 14:06 |

## Verify the Time and Date

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1.7 | IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room):<br>Date and time: 2024-04-26 at 14:06<br>**Note: All entries into this script or any logs should follow this common source of time.** | Y.Y. | 14:06 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 1 Step(s): 18 Page(s): 6<br>Date and time of the exception: 2024/04/26 @ 14:10<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 14:11. |

IW did not badge into Tier 4, thus had to leave tier 4 to badge back in.

## Open Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1.8 | CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.) | Y.Y. | 14:11 |
| 1.9 | SSC1 opens Safe #1 while shielding the combination from the camera.<br>**Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.** | Y.Y. | 14:12 |
| 1.10 | Perform the following steps to update the safe log:<br>a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. ✓<br>b) IW provides the pre-printed safe log to SSC1. ✓<br>c) SSC1 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. ✓<br>d) IW verifies the entry, then initials it. | Y.Y. | 14:13 |

## Access Equipment in Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1.11 | CA performs the indicated action for each item listed below with the following steps:<br>a) CAREFULLY remove each equipment TEB from the safe. ✓<br>b) Read aloud the TEB number, verify its integrity, then present it to the audit camera above. ✓<br>c) Place the equipment TEB on the cart as specified in the list below.<br>d) Write the date and time, then sign the safe log. ✓<br>e) IW verifies the completed safe log entries, then initials them. ✓<br><br>**HSM9E: TEB # BB02638477 (Place on Cart)** ✓<br>Last Verified: AT Ceremony 53-2 2024-03-27<br>**BHSM1E: TEB # BB02638476 (Place on Cart)** ✓<br>Last Verified: AT Ceremony 53-2 2024-03-27<br>**BHSM2E: TEB # BB02638475 (Place on Cart)** ✓<br>Last Verified: AT Ceremony 53-2 2024-03-27<br>**BHSM1W: TEB # BB02638474 (Place on Cart)** ✓<br>Last Verified: AT Ceremony 53-2 2024-03-27<br>**BHSM2W: TEB # BB02638473 (Place on Cart)** ✓<br>Last Verified: AT Ceremony 53-2 2024-03-27<br>**HSM10E: TEB # BB02638472 (Place on Cart)** ✓<br>Last Verified: AT Ceremony 53-2 2024-03-27<br><br>**Laptop4: TEB # BB81420078 (Place on Cart)** ✓<br>Last Verified: KSK Ceremony 51 2023-11-30<br><br>**OS media (release coen-1.1.0) + HSMFD: TEB # BB02639666 (Place on Cart)** ✓<br>Last Verified: KSK Ceremony 53-1 2024-04-25<br><br>**Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**<br>**The shelves in the equipment safe can slide in and out for ease of use.** | Y.Y. | 14:19 |

## Close Safe #1 (Tier 6, Equipment Safe) Exit Tier 5 (Safe Room)

| Step | Activity | Initials | Time |
|---|---|---|---|
| **1.12** | SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry then initials it. | Y.Y. | 14:19 |
| **1.13** | SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, then ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator adjacent to the Tier 5 (Safe Room) exit door is off. | Y.Y. | 14:20 |
| **1.14** | CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room). | Y.Y. | 14:20 |

# Act 2: Equipment Setup

The CA will set up the equipment by performing the following steps:

- Boot the laptop using the OS media (the laptop has no permanent storage device)
- Set up the printer
- Synchronize the laptop date and time
- Connect the HSMFD
- Start the log sessions
- Power ON the HSM (Tier 7)

## Laptop4 Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2.1 | CA performs the following steps to prepare each item listed below:<br>a) Remove the TEB from the cart, then place it on the ceremony table.<br>b) Inspect the equipment TEB for tamper evidence.<br>c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used.<br>d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.<br>**Laptop4: TEB # BB81420078 / Service Tag # 58SVSG2** ✓<br>Last Verified: KSK Ceremony 51 2023-11-30<br>**OS media (release coen-1.1.0) + HSMFD: TEB # BB02639666** ✓<br>Last Verified: KSK Ceremony 53-1 2024-04-25<br>**Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.** | Y.Y. | 14:25 |
| 2.2 | CA performs the following steps to confirm that no hard drive and battery are in the laptop:<br>a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty.<br>b) Open the latch on the left side of the laptop to confirm that the battery slot is empty. | Y.Y. | 14:26 |
| 2.3 | CA ensures the **lock switch** on the left side of the listed SD card is slid down to the lock position:<br>**OS media release coen-1.1.0**<br>**Copy # 2** | Y.Y. | 14:27 |
| 2.4 | CA performs the following steps to boot the laptop:<br>a) Connect the USB printer cable into the rear USB port of the laptop. ✓<br>b) Connect two USB HSM cables into the right-side USB ports of the laptop. ✓<br>c) Connect the external HDMI display cable into the left-side HDMI port of the laptop. ✓<br>d) Connect the power supply into the back of the laptop toward the CA'S left side. ✓<br>e) Insert the **OS media release coen-1.1.0 Copy # 2** into the right-side of the laptop. ✓<br>f) Switch it ON. ✓ | Y.Y. | 14:29 |
| 2.5 | CA verifies functionality of the external display and performs adjustments if necessary:<br>To change the font size of the terminal:<br>Click the **View** menu and select **Zoom In** or **Zoom Out**<br>To change the resolution of each screen:<br>Go to **Applications > Settings > Display** | Y.Y. | 14:29 |

## Invert the Terminal Text and Background Colors

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2.6 | CA performs the following steps to invert the text and background colors in the terminal:<br>a) Click the **"Edit"** menu, and select **"Preferences..."**<br>b) Click on the **"Colors"** tab at the top of the preferences menu.<br>c) Click the drop down arrow on the **"Presets"** menu, then select **"Black on White"**.<br>d) Close the **Terminal Preferences** window.<br>**Note: The colors are being inverted for optimized printouts.** | Y.Y. | 14:30 |

## OS Media coen-1.1.0 Checksum Verification

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2.7 | Using the **Commands** terminal window, CA executes the following steps:<br>a) Verify the byte count of the SD card matches the ISO size by running the following command:<br>`df -B1 /dev/sda`<br>b) Calculate the SHA-256 hash by executing:<br>`head -c 602406912 /dev/sda \| sha2wordlist`<br>c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.<br>**Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.**<br>SHA-256 hash:<br>**2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8**<br>PGP Words:<br>**blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous** ✓<br>**Note: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-2** | Y.Y. | 14:31 |

## Printer Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2.8 | CA confirms that the printer is switched ON: | Y.Y. | 14:32 |
| 2.9 | Using the **Commands** terminal window, CA executes the command below to configure the printer and print a test page:<br>`configure-printer` | Y.Y. | 14:32 |

## Date Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2.10 | Using the **Commands** terminal window, CA executes the command below to verify the date/time reasonably matches the ceremony clock.<br>`date`<br>If the date/time do not match, perform the following steps:<br>a) Execute `date -s "20240426 HH:MM:SS"` to set the time.<br>**where HH is two-digit hour, MM is two-digit minutes and SS is two-digit seconds.**<br>b) Execute `date` to confirm the date/time matches the clock. | Y.Y. | 14:33 |

## Connect the Ceremony 53-1 HSMFD

| Step | Activity | Initials | Time |
|---|---|---|---|
| **2.11** | CA plugs the **Ceremony 53-1 HSMFD** into a USB slot, then performs the steps below:<br>a) Wait for the file system window to appear.<br>b) Display the HSMFD contents to all participants.<br>c) Close the file system window. | Y.Y. | 14:34 |
| **2.12** | Using the **Commands** terminal window, CA executes the command below to calculate the SHA-256 hash of the HSMFD:<br>`hsmfd-hash -c`<br>IW confirms that the result matches the SHA-256 hash of the HSMFD using the printed HSMFD hash from the Ceremony 53-1 OS media bundle. | Y.Y. | 14:36 |

## Distribute Unused Ceremony 53-1 HSMFD

| Step | Activity | Initials | Time |
|---|---|---|---|
| **2.13** | CA gives the unused **Ceremony 53-1 HSMFD** and the sheet of paper with the printed HSMFD hash to RKOS. | Y.Y. | 14:36 |

## Start the Terminal Session Logging

| Step | Activity | Initials | Time |
|---|---|---|---|
| **2.14** | Using the **Commands** terminal window, CA executes the command below to change the working directory to HSMFD:<br>`cd /media/HSMFD` | Y.Y. | 14:37 |
| **2.15** | Using the **Commands** terminal window, CA executes the command below to log activities of the terminal window:<br>`script script-20240426.log` | Y.Y. | 14:37 |

# Act 3: New HSM (Tier 7) Introduction

The CA performs the new HSM introduction by executing the following steps:

- Inspect the HSM's Tamper Evident Bag for tamper evidence
- Power on HSM
- Recover HSM from Secure Transport Mode (STM)
- Generate and Clone Credentials
- Configure HSM Policies
- Initialize HSM
- Generate and verify a new KSK
- Place HSM in STM and power off
- Store the HSM inside of a Tamper Evident Bag
- Power off and disconnect remaining equipment
- Place HSM in Tier 6 (Equipment Safe #1)

## HSM Log Folder Creation

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.1 | Using the **Commands** terminal window, CA executes the command below to create a folder for the HSM(s) logs on the HSMFD:<br>`mkdir HSM9E BHSM1E BHSM2E BHSM1W BHSM2W HSM10E` | Y.Y. | 14:38 |

## HSM9E (Tier 7) Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.2 | CA performs the following steps to prepare **HSM9E**:<br>a) Remove the TEB from the cart and place it on the ceremony table.<br>b) Inspect the TEB for tamper evidence.<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used.<br>d) Remove and discard the TEB, then place **HSM9E** on its designated stand face down to allow the audit camera to record its serial number.<br>e) Read aloud the **HSM9E** serial number while IW verifies the information using the previous ceremony script where it was last used.<br>f) Flip **HSM9E** over face up in its designated stand.<br>**HSM9E: TEB # BB02638477 / Serial # 712482**<br>**Last Verified: AT Ceremony 53-2 2024-03-27** | Y.Y. | 14:41 |

## Power ON HSM9E (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.3 | CA performs the following steps to prepare **HSM9E**:<br>a) Plug a USB HSM cable into the USB-C port on the top of **HSM9E**.<br>b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility.<br>c) Wait for **HSM9E** to boot and confirm the device is in Secure Transport Mode (STM).<br>d) Verify the displayed HSM serial number on the screen matches **712482**.<br>**HSM9E: Serial # 712482** | Y.Y. | 14:42 |

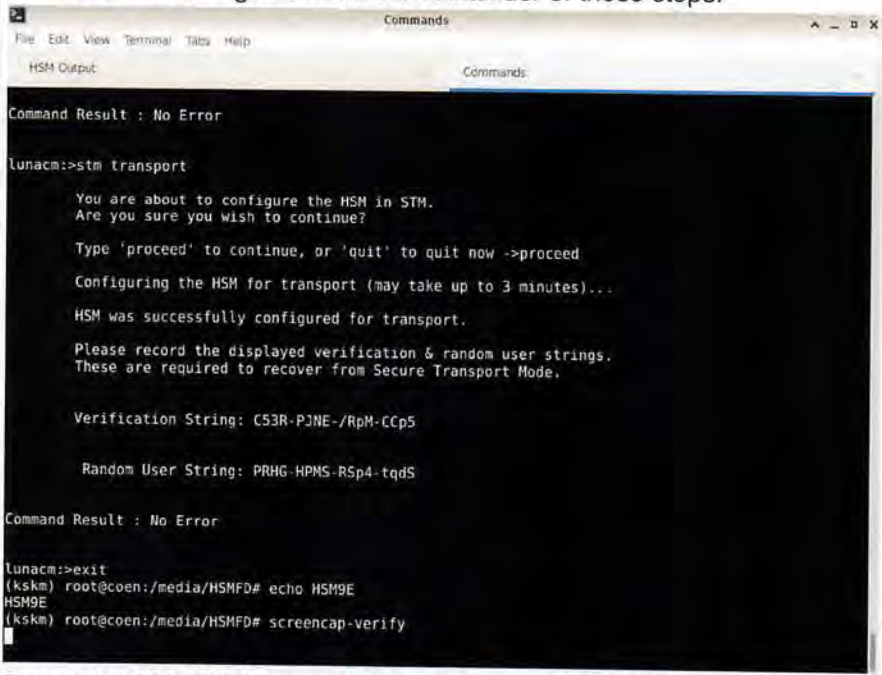
## Recover HSM9E (Tier 7) from Secure Transport Mode (STM)

<table>
<tr><th>Step</th><th>Activity</th><th>Initials</th><th>Time</th></tr>
<tr><td>3.4</td><td>

Using the **Commands** terminal window, CA executes the following steps to recover the HSM from STM:

a) Launch the **LunaCM** application:
`lunacm`

b) CA assigns half of the participants to confirm the strings displayed on the TV screen while the other half confirm the strings with the following image from the previous ceremony script.
Use this configuration for the remainder of these steps.



```
Command Result : No Error

lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: C53R-PJNE-/RpM-CCp5

         Random User String: PRHG-HPMS-RSp4-tqdS

Command Result : No Error

lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo HSM9E
HSM9E
(kskm) root@coen:/media/HSMFD# screencap-verify
```

**Screenshot of HSM9E STM placement during AT Ceremony 53-2 2024-03-27**

c) CA reads aloud the **Random User** string below while IW confirms that the result matches the printed screenshot from AT Ceremony 53-2 2024-03-27.
`PRHG-HPMS-RSp4-tqdS` ✓

d) Recover **HSM9E** from STM:
`stm recover -randomuserstring PRHG-HPMS-RSp4-tqdS`

**Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.**

e) IW confirms that the result matches the **Verification** string using the printed screenshot from AT Ceremony 53-2 2024-03-27.
`C53R-PJNE-/RpM-CCp5` ✓

f) Once the string is verified type `proceed`, then press enter to recover **HSM9E** from STM.

</td><td>Y.Y.</td><td>14:47</td></tr>
</table>

## Generate HSM9E (Tier 7) Audit Credentials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.5 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Initialize the **audit** role:<br>`role init -name au`<br>b) Type `proceed`, then press enter to continue. .<br>c) Follow the instructions on the **HSM9E touchscreen** to generate a 3 of 7 **audit** credential set:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Auditor..."** is displayed, select **"Create new quorum of iKeys"**, then press continue.<br>e) When **"How many iKeys will make up the full Auditor?"** is displayed, enter **7**, then press the ✓ in the lower right corner.<br>f) When **"How many iKeys will be required for authentication?"** is displayed, enter **3**, then press the ✓ in the lower right corner.<br>g) When **"Please insert first iKey"** is displayed, insert the **first iKey** in the **audit** set, then press continue. 1/1<br>h) When **"Create a new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>i) When **"Re-enter your new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>j) When **"First iKey successfully registered"** is displayed, remove the iKey, then press continue.<br>k) Repeat steps **g) to j)** for the 2nd ✓, 3rd ✓, 4th ✓, 5th ✓, 6th ✓, and 7th ✓ **audit** iKeys.<br>l) When **"Registration successful"** is displayed, press continue.<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 14:52 |

## Configure HSM9E (Tier 7) Audit Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.6 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in with the audit role:<br>`role login -name au`<br>b) Follow the instructions on the **HSM9E touchscreen** to perform **audit** authentication:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **audit** iKey, then press continue. 4<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 7<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 2<br>f) When **HSM9E** returns to its dashboard, remove the last iKey of the **audit** set.<br>g) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:<br>`audit time sync`<br>h) Set the filepath where log files are written:<br>`audit config path /media/HSMFD/HSM9E`<br>i) Set audit logging configuration:<br>`audit config evmask all,failure,success`<br>j) Type `proceed`, then press enter to continue.<br>k) Set audit logging rotation interval:<br>`audit config interval hourly@00`<br>l) Set audit logging maximum log file size:<br>`audit config size 4096k`<br>m) Show the audit logging configuration:<br>`audit config get`<br>n) Confirm with IW the output of the logging configuration matches with the list below:<br>`Current Logging Configuration`<br>`-----------------------------`<br>`event mask        : Log everything`<br>`rotation interval : hourly@ 0 minutes past the hour`<br>`rotation size (MB): 4`<br>`path to log       : /media/HSMFD/HSM9E`<br>`Command Result : No Error`<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 14:56 |

## Initialize HSM9E (Tier 7) Administrative Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.7 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **HSM9E** administrative partition:<br>`hsm init -label HSM9E -iped`<br>b) Type `proceed`, then press enter to continue.<br>c) Follow the instructions on the **HSM9E touchscreen** to generate a 3 of 7 **SO** and 5 of 7 **domain** credential set:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Security Officer..."** is displayed, select **"Create new Quorum of iKeys"**, then press continue.<br>e) When **"How many iKeys will make up the full Security Officer?"** is displayed, enter **7**, then press the ✓ in the lower right corner.<br>f) When **"How many iKeys will be required for authentication?"** is displayed, enter **3**, then press the ✓ in the lower right corner.<br>g) When **"Please insert first iKey"** is displayed, insert the first **SO** iKey, then press continue.<br>h) When **"Create a new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>i) When **"Re-enter your new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>j) When **"First iKey successfully registered"** is displayed, remove the iKey, then press continue. ✓<br>k) Repeat steps **g) to j)** for the 2nd ✓, 3rd ✓, 4th ✓, 5th ✓, 6th ✓, and 7th ✓ **SO** iKeys.<br>l) When **"Registration successful"** is displayed, press continue to automatically initiate **SO** authentication.<br>m) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 3<br>n) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>o) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** creation. 2<br>p) When **"Set up your domain..."** is displayed, remove the previous iKey, select **"Create new domain"**, then press continue.<br>q) When **"How many iKeys will make up the full Domain?"** is displayed, enter **7**, then press the ✓ in the lower right corner.<br>r) When **"How many iKeys will be required for authentication?"** is displayed, enter **5**, then press the ✓ in the lower right corner.<br>s) When **"Please insert first iKey"** is displayed, insert the first **domain** iKey, then press continue.<br>t) When **"Create a new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>u) When **"Re-enter your new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>v) When **"First iKey successfully set up"** is displayed, remove the iKey, then press continue. ✓<br>w) Repeat steps **s) to v)** for the 2nd ✓, 3rd ✓, 4th ✓, 5th ✓, 6th ✓, and 7th ✓ **domain** iKeys.<br>x) When **"Creation successful"** is displayed, press finish.<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:04 |

## Configure HSM9E (Tier 7) Global Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.8 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the **HSM9E** admin partition slot number:<br>`slot list`<br>b) Select the **HSM9E** admin partition slot:<br>`slot set -s 4`<br>c) Log in with the Security Officer role:<br>`role login -name so`<br>d) Follow the instructions on the **HSM9E touchscreen** to perform **SO** authentication:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 3<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>h) When **HSM9E** returns to its dashboard, remove the last iKey of the **SO** set.<br>i) Using the **LunaCM** terminal, activate FIPS mode:<br>`hsm changeHP -policy 12 -value 0`<br>j) Type `proceed`, then press enter to continue.<br>k) Disable PIN change after setup:<br>`hsm changeHP -policy 21 -value 0`<br>l) Verify **HSM9E** is in FIPS approved operation mode:<br>`hsm showinfo`<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:07 |

## Create HSM9E (Tier 7) Application Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.9 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Create the partition:<br>`partition create`<br>b) Verify the application partition slot number:<br>`slot list`<br>c) Select the application partition slot:<br>`slot set -s 3`<br>d) Initialize the application partition:<br>`partition init -label HSM9E_KSK-2024`<br>e) Type `proceed`, then press enter to continue.<br>f) Follow the instructions on the **HSM9E touchscreen** to register the **SO** and **domain** credential sets:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>g) When **"Register your Partition Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue.<br>h) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 4<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate Partition **SO** authentication. 6<br>k) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue.<br>l) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>m) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 7<br>n) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue.<br>o) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 7<br>p) When **"Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 3<br>q) When **"Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>r) When **"Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 6<br>s) When **"Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>t) When **HSM9E** returns to its dashboard, remove the last iKey of the **domain** set.<br>**Note 1: The "KE-CL" displayed on the dashboard indicates Key Export and Cloning are enabled.**<br>**Note 2: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:12 |

## Configure HSM9E (Tier 7) Partition Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| **3.10** | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in as the Partition Officer:<br>`role login -name po`<br>b) Follow the instructions on the **HSM9E touchscreen** to perform Partition **SO** authentication:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 2<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 4<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>f) When **HSM9E** returns to its dashboard, remove the last iKey of the **SO** set.<br>g) Using the **LunaCM** terminal, allow partition activation with PIN:<br>`partition changepolicy -policy 22 -value 1`<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:13 |

## Generate HSM9E (Tier 7) CO Credentials and PIN

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.11 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **CO** role:<br>`role init -name co`<br>b) Follow the instructions on the **HSM9E touchscreen** to generate a 3 of 7 **CO** credential set:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>c) When **"Register your Crypto Officer..."** is displayed, select **"Create new quorum of iKeys"**, then press continue.<br>d) When **"How many iKeys will make up the full Crypto Officer?"** is displayed, enter **7**, then press the ✓ in the lower right corner.<br>e) When **"How many iKeys will be required for authentication?"** is displayed, enter **3**, then press the ✓ in the lower right corner.<br>f) When **"Please insert first iKey"** is displayed, insert the first **CO** iKey, then press continue.<br>g) When **"Create a new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>h) When **"Re-enter your new PIN for this iKey"** is displayed, leave the input **blank**, then press the ✓ in the lower right corner.<br>i) When **"First iKey successfully registered"** is displayed, remove the iKey, then press continue.<br>j) Repeat steps **f) to i)** for the 2nd ✓, 3rd ✓, 4th ✓, 5th ✓, 6th ✓, and 7th ✓ **CO** iKeys.<br>k) When **"Registration successful"** is displayed, press continue.<br>l) Using the **LunaCM** terminal, configure a **CO** PIN:<br>`role createchallenge -name co`<br>m) When **"Enter new challenge secret:"** is displayed, type `11223344`, then press enter.<br>n) When **"Re-enter new challenge secret:"** is displayed, type `11223344`, then press enter.<br>o) Log out of **CO** role:<br>`role logout`<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:17 |

## Clone Recovery Key Share Holder CO iKeys

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.12 | CA clones the credential sets listed below as specified in sequential order, beginning with the **1st** and ending with the **7th** iKeys.<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>Using the **HSM9E touchscreen**, CA executes the following steps:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>a) Select the **Admin** tab at the top of the display.<br>b) Insert the **1st source** iKey to be cloned, then press **"Duplicate this iKey"**.<br>c) When **"Please insert a new iKey"** is displayed, remove the **1st source** iKey and give to IW to place it in its designated plastic case.<br>d) Take the **1st recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>e) When **"iKey duplicated"** is displayed, press continue, then the **1st recipient** iKey becomes the **2nd source** iKey, so select **"Duplicate this iKey"**.<br>f) When **"Please insert a new iKey"** is displayed, remove the **2nd source** iKey and give to IW to place it in its designated plastic case.<br>g) Take the **2nd recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>h) When **"iKey duplicated"** is displayed, press continue, remove the **2nd recipient** iKey, then place it on the credential stand.<br>i) Repeat steps **b) to h)** for the **2nd, 3rd, 4th, 5th, 6th, and 7th** iKeys in the **CO** credential sets.<br>j) Select the **Dashboard** tab at the top of the display.<br>1st **Source:** "RKSH CO SET **1**" **Recipient:** "RKSH CO SET **2**"<br>2nd **Source:** "RKSH CO SET **2**" **Recipient:** "TCR CO SET **1** Copy 1"<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:26 |

## Clone Recovery Key Share Holder Domain iKeys

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.13 | CA clones the credential sets listed below as specified in sequential order, beginning with the **1st** and ending with the **7th** iKeys.<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>Using the **HSM9E touchscreen**, CA executes the following steps:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>a) Select the **Admin** tab at the top of the display.<br>b) Insert the **1st source** iKey to be cloned, then press **"Duplicate this iKey"**.<br>c) When **"Please insert a new iKey"** is displayed, remove the **1st source** iKey and give to IW to place it in its designated plastic case.<br>d) Take the **1st recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>e) When **"iKey duplicated"** is displayed, press continue, then the **1st recipient** iKey becomes the **2nd source** iKey, so select **"Duplicate this iKey"**.<br>f) When **"Please insert a new iKey"** is displayed, remove the **2nd source** iKey and give to IW to place it in its designated plastic case.<br>g) Take the **2nd recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>h) When **"iKey duplicated"** is displayed, press continue, remove the **2nd recipient** iKey, then place it on the credential stand.<br>i) Repeat steps **b) to h)** for the **2nd, 3rd, 4th, 5th, 6th, and 7th** iKeys in the **Domain** credential sets.<br>j) Select the **Dashboard** tab at the top of the display.<br>1st **Source:** "RKSH Domain SET **1**" **Recipient:** "RKSH Domain SET **2**"<br>2nd **Source:** "RKSH Domain SET **2**" **Recipient:** "TCR Domain SET **1** Copy **1**"<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 15:32 |

## Place Recovery Key Share Holders' Credentials into TEBs

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.14 | The CA calls each of the RKSHs listed below sequentially to the ceremony table to perform the following steps:<br>a) CA asks the IW for the RKSH's designated new primary TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. ✓✓✓✓✓✓<br>b) CA asks the IW for the RKSH's designated new backup TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. ✓✓✓✓✓✓<br>c) CA places the backup TEB inside of the primary TEB in case the primary TEB is compromised in the future. ✓✓✓✓✓✓<br>d) CA places the RKSH note inside of the primary TEB, ensuring it's still legible through the bag. ✓✓✓✓✓✓<br>e) CA along with IW inspects the designated plastic credential case to ensure it contains the **CO** and **Domain** iKeys allocated to the RKSH. ✓✓✓✓✓<br>f) RKSH inspects the designated credential plastic case to ensure it contains their allocated **CO** and **Domain** iKeys. ✓✓✓✓✓✓<br>g) CA places the plastic case into its designated new TEB, then seals it. ✓✓✓✓✓✓<br>h) CA gives the IW sealing strips for post-ceremony inventory. ✓✓✓✓✓<br>i) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. ✓✓✓✓✓✓<br>j) CA initials the TEB with a ballpoint pen. ✓✓✓✓✓✓<br>k) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. ✓✓✓✓✓✓<br>l) RKSH inspects the TEB, verifies its contents, then initials it with a ballpoint pen. ✓✓✓✓✓✓<br>m) RKSH writes the date and time, signs the credential table of the IW's script, then IW initials the entry. ✓✓✓✓✓✓<br>n) RKSH returns to their seat with their TEB. ✓✓✓✓✓<br>o) Repeat steps for all the remaining RKSHs on the list. ✓<br><br>**RKSH1: Sebastian Castro**<br>**Luna Credential TEB # BB02638647** ✓<br>**Luna Credential Backup TEB # BB02638646** ✓<br><br>**RKSH2: Ondřej Surý**<br>**Luna Credential TEB # BB02639616** ✓<br>**Luna Credential Backup TEB # BB02639615** ✓<br><br>**RKSH3: Kristian Ørmen**<br>**Luna Credential TEB # BB02639614** ✓<br>**Luna Credential Backup TEB # BB02639613** ✓<br><br>**RKSH4: Jiankang Yao**<br>**Luna Credential TEB # BB02639612** ✓<br>**Luna Credential Backup TEB # BB02639611** ✓<br><br>**RKSH5: Bevil Wooding**<br>**Luna Credential TEB # BB02639610** ✓<br>**Luna Credential Backup TEB # BB02639609** ✓<br><br>**RKSH6: John Curran**<br>**Luna Credential TEB # BB02639608** ✓<br>**Luna Credential Backup TEB # BB02639607** ✓<br><br>**RKSH7: Dave Lawrence**<br>**Luna Credential TEB # BB02639606** ✓<br>**Luna Credential Backup TEB # BB02639605** ✓ | Y.Y. | 15:53 |

| TCR | TEB # | Printed Name | Signature | Date | Time | IW Initials |
|---|---|---|---|---|---|---|
| **RKSH1** | TEB # **BB02638647** | **Sebastian Castro** | | **2024 Apr** 26 | 15:37 | Y.Y. |
| **RKSH2** | TEB # **BB02639616** | **Ondřej Surý** | | **2024 Apr** 26 | 15:41 | Y.Y. |
| **RKSH3** | TEB # **BB02639614** | **Kristian Ørmen** | | **2024 Apr** 26 | 15 44 | Y.Y. |
| **RKSH4** | TEB # **BB02639612** | **Jiankang Yao** | Jiankang Yao | **2024 Apr** 26 | 15:46 | Y.Y. |
| **RKSH5** | TEB # **BB02639610** | **Bevil Wooding** | | **2024 Apr** 26 | 15·49 | Y.Y. |
| **RKSH6** | TEB # **BB02639608** | **John Curran** | | **2024 Apr** 26 | 15:51 | Y.Y. |
| **RKSH7** | TEB # **BB02639606** | **Dave Lawrence** | | **2024 Apr** 26 | 1553 | Y.Y. |

## Clone Crypto Officer CO iKeys

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.15 | CA clones the credential sets listed below as specified in sequential order, beginning with the **1st** and ending with the **7th** iKeys.<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>Using the **HSM9E touchscreen**, CA executes the following steps:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>a) Select the **Admin** tab at the top of the display. ✓<br>b) Insert the **1st source** iKey to be cloned, then press **"Duplicate this iKey"**. ✓<br>c) When **"Please insert a new iKey"** is displayed, remove the **1st source** iKey and give to IW to place it in its designated plastic case. ✓<br>d) Take the **1st recipient** iKey from the credential stand, insert it into the HSM, then press continue. ✓<br>e) When **"iKey duplicated"** is displayed, press continue, then the **1st recipient** iKey becomes the **2nd source** iKey, so select **"Duplicate this iKey"**. ✓<br>f) When **"Please insert a new iKey"** is displayed, remove the **2nd source** iKey and give to IW to place it in its designated plastic case. ✓<br>g) Take the **2nd recipient** iKey from the credential stand, insert it into the HSM, then press continue. ✓<br>h) When **"iKey duplicated"** is displayed, press continue, then the **2nd recipient** iKey becomes the **3rd source** iKey, so select **"Duplicate this iKey"**. ✓<br>i) When **"Please insert a new iKey"** is displayed, take the **3rd recipient** iKey from the credential stand, remove the **3rd source** iKey from the HSM and place it on the credential stand. ✓<br>j) Insert the **3rd recipient** iKey into the HSM, then press continue. ✓<br>k) When **"iKey duplicated"** is displayed, press continue, remove the **3rd recipient** iKey, and place it on the credential stand. ✓<br>l) Repeat steps **b) to h)** for the **2nd, 3rd, 4th, 5th, 6th, and 7th** iKeys in the **CO** credential sets.<br>m) Select the **Dashboard** tab at the top of the display.<br><br>1st **Source:** "TCR CO SET **1** Copy 1" **Recipient:** "TCR CO SET **2** Copy 1"<br>2nd **Source:** "TCR CO SET **2** Copy 1" **Recipient:** "TCR CO SET **1** Copy 2"<br>3rd **Source:** "TCR CO SET **1** Copy 2" **Recipient:** "TCR CO SET **2** Copy 2"<br><br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 16:05 |

## Clone Crypto Officer SO iKeys

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.16 | CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>Using the **HSM9E touchscreen**, CA executes the following steps:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>a) Select the **Admin** tab at the top of the display. ✓<br>b) Insert the **1st source** iKey to be cloned, then press **"Duplicate this iKey"**.<br>c) When **"Please insert a new iKey"** is displayed, remove the **1st source** iKey and give to IW to place it in its designated plastic case.<br>d) Take the **1st recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>e) When **"iKey duplicated"** is displayed, press continue, then the **1st recipient** iKey becomes the **2nd source** iKey, so select **"Duplicate this iKey"**.<br>f) When **"Please insert a new iKey"** is displayed, remove the **2nd source** iKey and give to IW to place it in its designated plastic case.<br>g) Take the **2nd recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>h) When **"iKey duplicated"** is displayed, press continue, then the **2nd recipient** iKey becomes the **3rd source** iKey, so select **"Duplicate this iKey"**.<br>i) When **"Please insert a new iKey"** is displayed, take the **3rd recipient** iKey from the credential stand, remove the **3rd source** iKey from the HSM and place it on the credential stand.<br>j) Insert the **3rd recipient** iKey into the HSM, then press continue.<br>k) When **"iKey duplicated"** is displayed, press continue, remove the **3rd recipient** iKey, and place it on the credential stand.<br>l) Repeat steps **b) to h)** for the **2nd, 3rd, 4th, 5th, 6th, and 7th** iKeys in the **SO** credential sets.<br>m) Select the **Dashboard** tab at the top of the display.<br>1st **Source:** "TCR SO SET **1** Copy 1" **Recipient:** "TCR SO SET **2** Copy 1"<br>2nd **Source:** "TCR SO SET **2** Copy 1" **Recipient:** "TCR SO SET **1** Copy 2"<br>3rd **Source:** "TCR SO SET **1** Copy 2" **Recipient:** "TCR SO SET **2** Copy 2"<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 16:12 |

## Clone Crypto Officer Audit iKeys

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.17 | CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>Using the **HSM9E touchscreen**, CA executes the following steps:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>a) Select the **Admin** tab at the top of the display. ✓<br>b) Insert the **1st source** iKey to be cloned, then press **"Duplicate this iKey"**.<br>c) When **"Please insert a new iKey"** is displayed, remove the **1st source** iKey and give to IW to place it in its designated plastic case.<br>d) Take the **1st recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>e) When **"iKey duplicated"** is displayed, press continue, then the **1st recipient** iKey becomes the **2nd source** iKey, so select **"Duplicate this iKey"**.<br>f) When **"Please insert a new iKey"** is displayed, remove the **2nd source** iKey and give to IW to place it in its designated plastic case.<br>g) Take the **2nd recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>h) When **"iKey duplicated"** is displayed, press continue, then the **2nd recipient** iKey becomes the **3rd source** iKey, so select **"Duplicate this iKey"**.<br>i) When **"Please insert a new iKey"** is displayed, take the **3rd recipient** iKey from the credential stand, remove the **3rd source** iKey from the HSM and place it on the credential stand.<br>j) Insert the **3rd recipient** iKey into the HSM, then press continue.<br>k) When **"iKey duplicated"** is displayed, press continue, remove the **3rd recipient** iKey, and place it on the credential stand.<br>l) Repeat steps **b) to h)** for the **2nd, 3rd, 4th, 5th, 6th, and 7th** iKeys in the **Audit** credential sets.<br>m) Select the **Dashboard** tab at the top of the display. ✓<br>1st **Source:** "TCR Audit SET **1** Copy 1" **Recipient:** "TCR Audit SET **2** Copy 1"<br>2nd **Source:** "TCR Audit SET **2** Copy 1" **Recipient:** "TCR Audit SET **1** Copy 2"<br>3rd **Source:** "TCR Audit SET **1** Copy 2" **Recipient:** "TCR Audit SET **2** Copy 2"<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 16:19 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 3 Step(s): 18 (K) 7 Page(s): 27<br>Date and time of the exception: 2024/04/26 @ 16:27.<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 16:28 |

~~For the~~

CA removed the key before pressing "continue" for the key 7. The Luna asked if we want to cancel operation, which we did.

## Clone Crypto Officer Domain iKeys

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.18 | CA clones the credential sets listed below as specified in sequential order, beginning with the **1st** and ending with the **7th** iKeys.<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>Using the **HSM9E touchscreen**, CA executes the following steps:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>a) Select the **Admin** tab at the top of the display. ✓<br>b) Insert the **1st source** iKey to be cloned, then press **"Duplicate this iKey"**.<br>c) When **"Please insert a new iKey"** is displayed, remove the **1st source** iKey and give to IW to place it in its designated plastic case.<br>d) Take the **1st recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>e) When **"iKey duplicated"** is displayed, press continue, then the **1st recipient** iKey becomes the **2nd source** iKey, so select **"Duplicate this iKey"**.<br>f) When **"Please insert a new iKey"** is displayed, remove the **2nd source** iKey and give to IW to place it in its designated plastic case.<br>g) Take the **2nd recipient** iKey from the credential stand, insert it into the HSM, then press continue.<br>h) When **"iKey duplicated"** is displayed, press continue, then the **2nd recipient** iKey becomes the **3rd source** iKey, so select **"Duplicate this iKey"**.<br>i) When **"Please insert a new iKey"** is displayed, take the **3rd recipient** iKey from the credential stand, remove the **3rd source** iKey from the HSM and place it on the credential stand.<br>j) Insert the **3rd recipient** iKey into the HSM, then press continue.<br>k) When **"iKey duplicated"** is displayed, press continue, remove the **3rd recipient** iKey, and place it on the credential stand.<br>l) Repeat steps **b) to h)** for the **2nd, 3rd, 4th, 5th, 6th, and 7th** iKeys in the **Domain** credential sets.<br>m) Select the **Dashboard** tab at the top of the display.<br>1st **Source:** "TCR Domain SET **1** Copy 1" **Recipient:** "TCR Domain SET **2** Copy 1"<br>2nd **Source:** "TCR Domain SET **2** Copy 1" **Recipient:** "TCR Domain SET **1** Copy 2"<br>3rd **Source:** "TCR Domain SET **1** Copy 2" **Recipient:** "TCR Domain SET **2** Copy 2"<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 16:28 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 3 Step(s): 19 Page(s): 28<br>Date and time of the exception: 2024/04/26 @ 16:40<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 16:41 |

Ólafur Guðmundsson was present therefore he came to the table to verify the contents of the cases, verified the TEB, then initialed it.

## Place KMF West Crypto Officers' Credentials into TEBs

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.19 | The CA prepares the KMF West Crypto Officer credentials by performing the following steps for each entry listed below:<br>a) CA asks the IW for the KMF West Crypto Officer's designated new TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. ✓✓✓✓✓✓✓<br>b) CA along with IW inspects the designated plastic credential case to ensure it contains the iKeys allocated to the KMF West Crypto Officer. ✓✓✓✓✓✓✓<br>c) CA places the plastic case into its designated new TEB, then seals it. ✓✓✓✓✓✓✓<br>d) CA gives the IW sealing strips for post-ceremony inventory. ✓✓✓✓✓✓✓<br>e) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. ✓✓✓✓✓✓✓<br>f) CA initials the TEB with a ballpoint pen. ✓✓✓✓✓✓✓<br>g) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. ✓✓✓✓✓✓✓<br>h) CA gives the TEB to IW to set aside pending the next step. ✓✓✓✓✓✓✓<br>**CO1: Arbogast Fabian**<br>**TEB # BB02639636** ✓<br>**CO2: Ralf Weber**<br>**TEB # BB02639635** ✓<br>**CO3: João Damas**<br>**TEB # BB02639634** ✓<br>**CO4: Carlos Martinez**<br>**TEB # BB02639633** ✓<br>**CO5: Ólafur Guðmundsson**<br>**TEB # BB02639632** ✓<br>**CO6: Jorge Etges**<br>**TEB # BB02639631** ✓<br>**CO7: Subramanian Moonesamy**<br>**TEB # BB02639630** ✓ | Y.Y. | 16:41 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 3 Step(s): 20 - H Page(s): 29<br>Date and time of the exception: 2024/04/26@ 16:52<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 16:53 |

For overwrap #2 TEB, it was too small thus we used a new, bigger TEB BB51184307 instead.

## Place KMF West Crypto Officers' Individual TEBs into Overwrap TEBs for Transport.

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.20 | The CA perform the following steps to place the KMF West Crypto Officer Credentials into overwrap TEBs for transport:<br>a) CA asks the IW for the for Credential Overwrap **#1**, then reads the TEB number and description aloud while IW verifies it matches the information below. ✓<br>b) CA asks the IW for the **1st, 2nd, and 3rd** KMF West Coast Crypto Officer Credential TEBs, places them inside of Credential Overwrap TEB **#1**, then seals it. ✓<br>c) CA gives the IW sealing strips for post-ceremony inventory. ✓<br>d) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. ✓<br>e) CA initials the TEB with a ballpoint pen. ✓<br>f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. ✓<br>g) RKOS initials the TEB, then IW takes custody of the Credential Overwrap TEB **#1** for transit to KMF West. ✓<br>* h) CA asks the IW for the for Credential Overwrap **#2**, then reads the TEB number and description aloud while IW verifies it matches the information below. ✓<br>i) CA asks the IW for the **4th, 5th, 6th, and 7th** KMF West Coast Crypto Officer Credential TEBs, places them inside of Credential Overwrap TEB **#2**, then seals it. ✓<br>j) CA gives the IW sealing strips for post-ceremony inventory. ✓<br>k) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. ✓<br>l) CA initials the TEB with a ballpoint pen. ✓<br>m) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. ✓<br>n) RKOS initials the TEB, then RKOS takes custody of the Credential Overwrap TEB **#2** for transit to KMF West. ✓<br><br>**Credential Overwrap #1 TEB # BB02639629** ✓<br>**Credential Overwrap #2 TEB # ~~BB02639628~~** | Y.Y. | 16:53 |

BB51184307

## Lunch Break

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.21 | CA and IW ensure all ceremony participants are escorted out of Tier 4 (Ceremony Room). Target break window is 30 minutes.<br>a) Audit Cameras are never obstructed.<br>b) Live stream audio is muted until the ceremony resumes.<br><br>RKOS will escort each group of participants out of the ceremony room for the ceremony break. | Y.Y. | 16:54 |
| 3.22 | Once all of the groups have returned to Tier 4 (Ceremony Room) from the break, CA ensures live stream audio is enabled, all participants are present by performing a roll call, then resumes the ceremony. | Y.Y. | 17:27 |

**kskm-keymaster-20240426-173035-995.log**

```
Loaded configuration from file ksrsigner.yaml SHA-256 5a2ff2646e14ab6883fd972faf9baf1cd91c237a01df738
b1f9288a6449ed3ec WORDS enlist combustion uproot getaway goldfish belowground rhythm gravity Mohawk W
yoming preshrunk combustion rocker Norwegian rocker Brazilian sugar Brazilian blowtorch infancy absur
d therapist hockey Medusa billiard misnomer newborn paragon crumpled onlooker stapler unicorn
Configuration validated
Initializing PKCS#11 module luna using /usr/safenet/lunaclient/lib/libCryptoki2_64.so
HSM First slot:         HSM9E_KSK-2024
HSM ManufacturerID:
HSM Model:              Luna G7
HSM Serial:             1658876115494
Generate key
Generated key: key_label=Kmyv6jo alg=RSA bits=2048 exp=65537
Generated key Kmyv6jo has key tag 38696 for algorithm=AlgorithmDNSSEC.RSASHA256, flags=0x101
Generated key Kmyv6jo has key tag 38824 with the REVOKE bit set (flags 0x181)
DS record for generated key:
. IN DS 38696 8 2 683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16
>> frighten crucifix button Apollo spheroid megaton puppy hideaway brickyard bottomless deadbolt pion
eer lockup hydraulic atlas bottomless breakup microscope allow detector ancient frequency Burbank dic
tator cleanup Virginia crumpled Pandora slowdown Wichita briefcase bodyguard
```

```
Loaded configuration from file ksrsigner.yaml SHA-256 5a2ff2646e14ab6883fd972faf9baf1cd91c237a01df738
b1f9288a6449ed3ec WORDS enlist combustion uproot getaway goldfish belowground rhythm gravity Mohawk W
yoming preshrunk combustion rocker Norwegian rocker Brazilian sugar Brazilian blowtorch infancy absur
d therapist hockey Medusa billiard misnomer newborn paragon crumpled onlooker stapler unicorn
Configuration validated
Initializing PKCS#11 module luna using /usr/safenet/lunaclient/lib/libCryptoki2_64.so
HSM First slot:      HSM9E_KSK-2024
HSM ManufacturerID:
HSM Model:           Luna G7
HSM Serial:          1658876115494
Show HSM inventory
Key inventory:
HSM luna:
  Slot 3:
    Signing key pairs:
      Kmyv6jo alg=RSA bits=2048 exp=65537 -- Matching KSK not found in configuration
```

## KSK Generation

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.23 | Using the **LunaCM** terminal, CA executes the following steps to generate a new KSK:<br>a) Log in with the Crypto Officer role:<br>`role login -name co`<br>b) When **"enter password"** is displayed, enter the **secret** password:<br>`11223344`<br>c) Follow the instructions on the **HSM9E touchscreen** to perform **CO** authentication:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>d) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 7<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 5<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 2<br>g) When **HSM9E** returns to its dashboard, remove the last iKey of the **CO** set.<br>h) Exit the **LunaCM** terminal window by typing the following command:<br>`exit`<br>i) Using the **Commands** terminal window, execute the command below to change the working directory:<br>`cd /media/HSMFD/KSK53-2`<br>j) Initiate key generation with the following multi-line command:<br>`kskm-keymaster --hsm luna keygen`<br>`--algorithm RSASHA256 --size 2048`<br>k) Verify the presence of the keypair created previously:<br>`kskm-keymaster --hsm luna inventory`<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 17:31 |

## KSK Key Tag Verification

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.24 | CA verifies that the new KSK's key tag and the key tag with the revoke bit set are different from the previous KSK's key tag:<br>`KSK   Label    Key Tag   Revoke`<br>`2010  Kjqmt7v   19036    19164`<br>`2017  Klajeyz   20326    20454`<br>`2023  Kmrfl3b   46211    46339` | Y.Y. | 17:32 |

## Print Copies of the KSK Generation Log

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.25 | Using the **Commands** terminal window, the CA executes the commands below to print the KSK generation log:<br>`printlog kskm-keymaster-202404*.log X`<br>**Note: Replace "X" with the quantity of copies needed for the participants.** | Y.Y | ~~17:37~~<br>17:40 |
| 3.26 | IW attaches two copies of the required KSK generation log to their script. | Y.Y. | 17:40 |

## Record Key Label

| Step | Activity | Initials | Time |
|---|---|---|---|
| **3.27** | IW records the key label:<br>**Root KSK 2024 Label**: Kmyv6jo | Y.Y. | 17:41 |

## BHSM1E (Tier 7) Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| **3.28** | CA performs the following steps to prepare **BHSM1E**:<br>a) Remove the TEB from the cart and place it on the ceremony table ✓<br>b) Inspect the TEB for tamper evidence. ✓<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>d) Remove and discard the TEB, then place **BHSM1E** on its designated stand face down to allow the audit camera to record its serial number. ✓<br>e) Read aloud the **BHSM1E** serial number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>f) Flip **BHSM1E** over face up in its designated stand. ✓<br>**BHSM1E: TEB # BB02638476 ✓ / Serial # 706530**<br>**Last Verified: AT Ceremony 53-2 2024-03-27** | Y.Y. | 17:43 |

## Power ON BHSM1E (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| **3.29** | CA performs the following steps to prepare **BHSM1E**:<br>a) Plug a USB HSM cable into the USB-C port on the top of **BHSM1E**. ✓<br>b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. ✓<br>c) Wait for **BHSM1E** to boot and confirm the device is in Secure Transport Mode (STM). ✓<br>d) Verify the displayed HSM serial number on the screen matches **706530**. ✓<br>**BHSM1E: Serial # 706530** | Y.Y. | 17:45 |

## Recover BHSM1E (Tier 7) from Secure Transport Mode (STM)

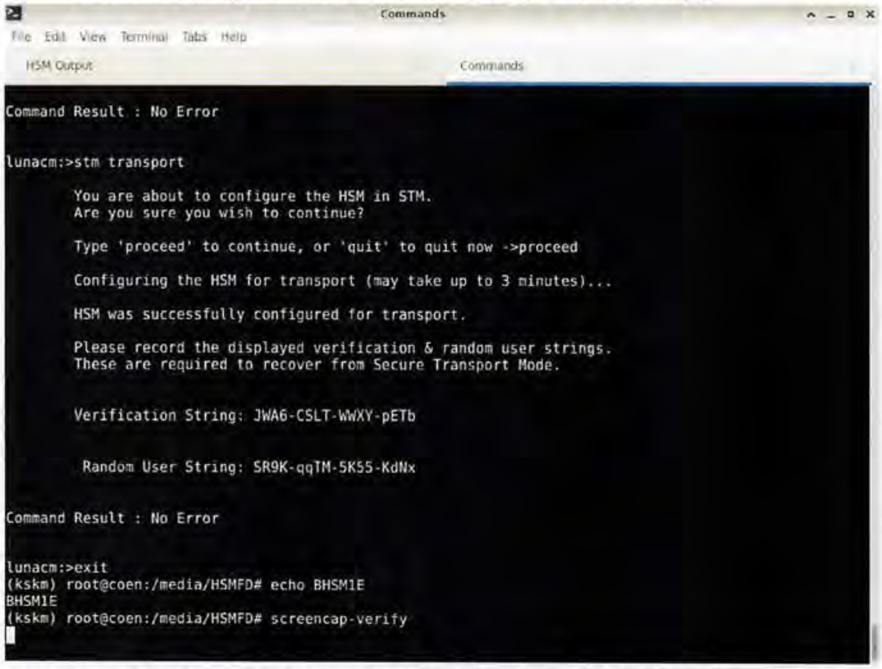
<table>
<tr><th>Step</th><th>Activity</th><th>Initials</th><th>Time</th></tr>
<tr><td>3.30</td><td>

Using the **Commands** terminal window, CA executes the following steps to recover the HSM from STM:

a) Launch the **LunaCM** application:
`lunacm`

b) Select the **BHSM1E: Serial # 706530** admin partition slot:
`slot set -s 105`

c) CA assigns half of the participants to confirm the strings displayed on the TV screen while the other half confirm the strings with the following image from the previous ceremony script.
Use this configuration for the remainder of these steps.



```
Command Result : No Error


lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: JWA6-CSLT-WWXY-pETb


         Random User String: SR9K-qqTM-5K55-KdNx


Command Result : No Error


lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo BHSM1E
BHSM1E
(kskm) root@coen:/media/HSMFD# screencap-verify
```

**Screenshot of BHSM1E STM placement during AT Ceremony 53-2 2024-03-27**

d) CA reads aloud the **Random User** string below while IW confirms that the result matches the printed screenshot from AT Ceremony 53-2 2024-03-27.
`SR9K-qqTM-5K55-KdNx` ✓

e) Recover **BHSM1E** from STM:
`stm recover -randomuserstring SR9K-qqTM-5K55-KdNx` ✓

**Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.**

f) IW confirms that the result matches the **Verification** string using the printed screenshot from AT Ceremony 53-2 2024-03-27.
`JWA6-CSLT-WWXY-pETb` ✓

g) Once the string is verified type `proceed`, then press enter to recover **BHSM1E** from STM. ✓

</td><td>Y.Y.</td><td>17:50</td></tr>
</table>

## Register BHSM1E (Tier 7) Audit Credentials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.31 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Initialize the **audit** role:<br>`role init -name au` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM1E touchscreen** to register a 3 of 7 **audit** credential set: ✓<br>**Note: If the BHSM1E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Auditor..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert **audit iKey 1 of 7**, then press continue. ✓<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **audit iKey 2 of 7**, then press continue. ✓<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert **audit iKey 3 of 7**, then press continue. ✓<br>h) When **BHSM1E** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y-Y. | 17:52 |

## Configure BHSM1E (Tier 7) Audit Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.32 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in with the audit role:<br>`role login -name au` ✓<br>b) Follow the instructions on the **BHSM1E touchscreen** to perform **audit** authentication:<br>**Note: If the BHSM1E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, insert **audit iKey 4 of 7**, then press continue. ✓<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **audit iKey 5 of 7**, then press continue. ✓<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert **audit iKey 6 of 7**, then press continue. ✓<br>f) When **BHSM1E** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>g) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:<br>`audit time sync` ✓<br>h) Set the filepath where log files are written:<br>`audit config path /media/HSMFD/BHSM1E` ✓<br>i) Set audit logging configuration:<br>`audit config evmask all,failure,success` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Set audit logging rotation interval:<br>`audit config interval hourly@00` ✓<br>l) Set audit logging maximum log file size:<br>`audit config size 4096k` ✓<br>m) Show the audit logging configuration:<br>`audit config get` ✓<br>n) Confirm with IW the output of the logging configuration matches with the list below:<br>`Current Logging Configuration`<br>`-----------------------------`<br>`event mask        : Log everything`<br>`rotation interval : hourly@ 0 minutes past the hour`<br>`rotation size (MB): 4`<br>`path to log       : /media/HSMFD/BHSM1E`<br>`Command Result : No Error` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 17:55 |

## Initialize BHSM1E (Tier 7) Administrative Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.33 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **BHSM1E** administrative partition:<br>`hsm init -label BHSM1E -iped` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM1E touchscreen** to register a 3 of 7 **SO** and 5 of 7 **domain** credential set: ✓<br>**Note: If the BHSM1E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue.<br>e) When **"Please insert first iKey"** is displayed, insert **SO iKey 1 of 7**, then press continue. ✓<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **SO iKey 2 of 7**, then press continue. ✓<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert **SO iKey 3 of 7**, then press continue to automatically initiate **SO** authentication. ✓<br>h) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey, insert **SO iKey 4 of 7**, then press continue. ✓<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey, insert **SO iKey 5 of 7**, then press continue to initiate **domain** registration. ✓<br>k) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>l) When **"Please insert first iKey"** is displayed, insert **domain iKey 1 of 7**, then press continue. ✓<br>m) When "**Please insert iKey 2 of 5**" is displayed, remove the previous iKey and insert **domain iKey 2 of 7**, then press continue. ✓<br>n) When "**Please insert iKey 3 of 5**" is displayed, remove the previous iKey and insert **domain iKey 3 of 7**, then press continue. ✓<br>o) When "**Please insert iKey 4 of 5**" is displayed, remove the previous iKey and insert **domain iKey 4 of 7**, then press continue. ✓<br>p) When "**Please insert iKey 5 of 5**" is displayed, remove the previous iKey and insert **domain iKey 5 of 7**, then press continue. ✓<br>q) When **BHSM1E** returns to its dashboard, remove the last iKey of the **domain** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 17:58 |

## Configure BHSM1E (Tier 7) Global Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.34 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the **BHSM1E** admin partition slot number:<br>`slot list` ✓<br>b) Select the **BHSM1E** admin partition slot:<br>`slot set -s 105` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so` ✓<br>d) Follow the instructions on the **BHSM1E touchscreen** to perform **SO** authentication:<br>**Note: If the BHSM1E touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert **SO iKey 6 of 7**, then press continue. ✓<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **SO iKey 7 of 7**, then press continue. ✓<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>h) When **BHSM1E** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, activate FIPS mode:<br>`hsm changehsmpolicy -policy 55 -value 1` ✓<br>j) Verify **BHSM1E** is in FIPS approved operation mode:<br>`hsm showinfo` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:00 |

## Back Up KSK Key Pair to BHSM1E (Tier 7) 1/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.35 | Using the **LunaCM** terminal, CA executes the following steps to perform **CO** authentication:<br>a) Verify the application partition slot number:<br>`slot list` ✓<br>b) Select the HSM's application partition slot:<br>`slot set -s 3` ✓<br>c) Log in with the Crypto Officer role:<br>`role login -name co` ✓<br>d) When **"enter password"** is displayed, enter the **secret** password:<br>`11223344` ✓<br>e) Show the KSK key pair:<br>`partition contents` ✓<br>f) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 18:02 |

# Back Up KSK Key Pair to BHSM1E (Tier 7) 2/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.36 | Using the **LunaCM** terminal, CA executes the following steps to back up KSK key pair:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initiate the backup from the HSM application partition to **BHSM1E**:<br>`partition archive backup -slot 105 -partition KSK-2024` ✓<br>b) Follow the instructions on the **BHSM1E touchscreen** to register and authenticate **SO**, Partition **SO**, **domain**, and **CO** credential sets: ✓<br>**Note: If the BHSM1E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, begin **SO** registration by inserting a randomly selected **SO** iKey, then press continue. 3<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 4<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate Partition **SO** registration. 7<br>f) When **"Register your Partition Security Officer...** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>g) When **"Please insert first iKey"** is displayed, leave the current iKey inserted, then press continue. ✓<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate Partition **SO** authentication. 5<br>j) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>k) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>l) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 6<br>*Continued on next page* | Y.Y. | 18:08 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 3 Step(s): 37-a Page(s): 38<br>Date and time of the exception: 2024/04/26 @ 18:15<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 18:15 |

CA did not follow the instruction on step 37a) by not remaving the key first before selecting "Join Existing domain". CA fixed the issue and there was no problem

## Back Up KSK Key Pair to BHSM1E (Tier 7) 2/3 (Continued)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.37 | a) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>b) When **"Please insert first iKey"** is displayed, insert **domain iKey 6 of 7**, then press continue. ✓<br>c) When **"Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert **domain iKey 7 of 7**, then press continue. ✓<br>d) When **"Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 5<br>e) When **"Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>f) When **"Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue to automatically initiate Partition **SO** authentication. 1<br>g) When **"Please ensure an iKey is inserted"** is displayed, remove the previous iKey and insert a randomly selected **SO** iKey, then press continue. 2<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 3<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **CO** registration. 6<br>j) When **"Register your Crypto Officer"** is displayed, remove the last iKey from the previous set, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>k) When **"Please insert first iKey"** is displayed, insert **CO iKey 1 of 7**, then press continue. ✓<br>l) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **CO iKey 2 of 7**, then press continue. ✓<br>m) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert **CO iKey 3 of 7**, then press continue to automatically initiate **CO** authentication. ✓<br>n) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>o) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **CO iKey 4 of 7**, then press continue. ✓<br>p) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert **CO iKey 5 of 7**, then press continue. ✓<br>q) When **BHSM1E** returns to its dashboard, remove the last iKey of the **CO** set. ✓ | Y.Y. | 18:~~13~~<br>15 |

## Back Up KSK Key Pair to BHSM1E (Tier 7) 3/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.38 | Using the **LunaCM** terminal, CA executes the following steps to verify the KSK key pair:<br>a) List the backups in **BHSM1E** by specifying **BHSM1E's** slot number:<br>`partition archive list -slot 105` ✓<br>b) List the contents of the backups in **BHSM1E**:<br>`partition archive contents -slot 105 -partition KSK-2024` ✓<br>c) Follow the instructions on the **BHSM1E touchscreen** to perform **CO** authentication:<br>**Note: If the BHSM1E touchscreen is off, tap it once to activate the display.**<br>d) When **"Please ensure an iKey is inserted"** is displayed, insert **CO iKey 6 of 7**, then press continue. ✓<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert **CO iKey 7 of 7**, then press continue. ✓<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. ✓<br>g) When **BHSM1E** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>h) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 18:17 |

## Place BHSM1E (Tier 7) in the TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.39 | CA performs the following steps to prepare **BHSM1E** for storage:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Unplug the HSM cable from the upper USB-C port of **BHSM1E**.<br>c) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below.<br>d) Read aloud the HSM serial number while the IW verifies it matches the information below.<br>e) Place the HSM into its designated new TEB, then seal it. ✓<br>f) Give IW the sealing strips for post-ceremony inventory. ✓<br>g) Place the HSM onto its designated space on the ceremony table visible to the audit camera. ✓<br>h) Initial the TEB along with IW using a ballpoint pen. ✓<br>i) Place the HSM TEB on the cart. ✓<br><br>**BHSM1E: TEB # BB02639622 ✓ / Serial # 706530 ✓** | Y.Y. | 18:19 |

## BHSM2E (Tier 7) Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.40 | CA performs the following steps to prepare **BHSM2E**:<br>a) Remove the TEB from the cart and place it on the ceremony table. ✓<br>b) Inspect the TEB for tamper evidence. ✓<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>d) Remove and discard the TEB, then place **BHSM2E** on its designated stand face down to allow the audit camera to record its serial number. ✓<br>e) Read aloud the **BHSM2E** serial number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>f) Flip **BHSM2E** over face up in its designated stand. ✓<br><br>**BHSM2E: TEB # BB02638475 / Serial # 718029**<br>**Last Verified: AT Ceremony 53-2 2024-03-27** | Y.Y. | 18:21 |

## Power ON BHSM2E (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.41 | CA performs the following steps to prepare **BHSM2E**:<br>a) Plug a USB HSM cable into the USB-C port on the top of **BHSM2E**. ✓<br>b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility.<br>c) Wait for **BHSM2E** to boot and confirm the device is in Secure Transport Mode (STM). ✓<br>d) Verify the displayed HSM serial number on the screen matches **718029**. ✓<br><br>**BHSM2E: Serial # 718029** ✓ | Y.Y. | 18:22 |

# Recover BHSM2E (Tier 7) from Secure Transport Mode (STM)

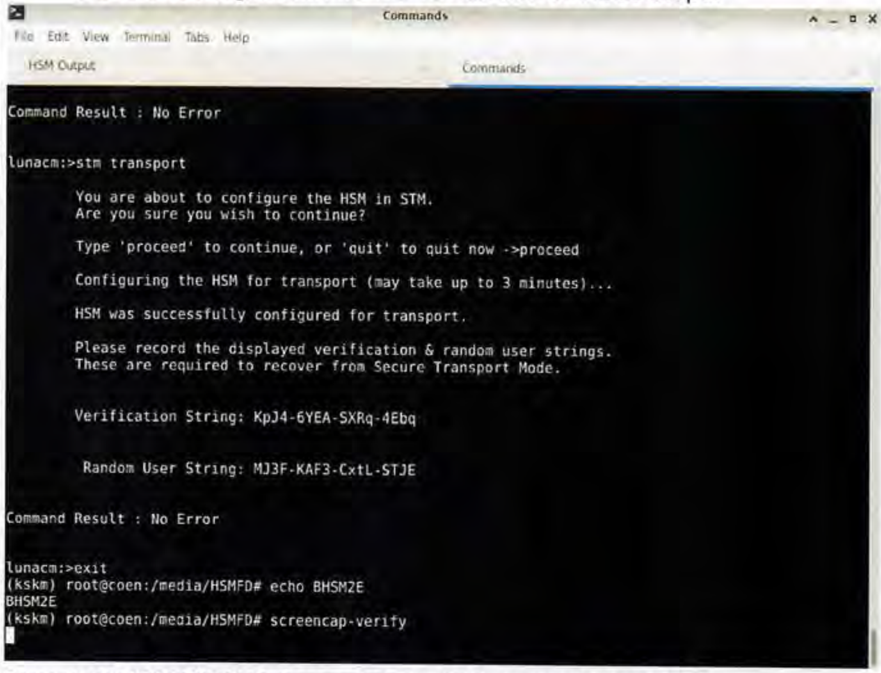
<table>
<tr><th>Step</th><th>Activity</th><th>Initials</th><th>Time</th></tr>
<tr><td>3.42</td><td>

Using the **Commands** terminal window, CA executes the following steps to recover the HSM from STM:

a) Launch the **LunaCM** application:
`lunacm` ✓

b) Select the **BHSM2E: Serial # 718029** admin partition slot:
`slot set -s 105` ✓

c) CA assigns half of the participants to confirm the strings displayed on the TV screen while the other half confirm the strings with the following image from the previous ceremony script.
Use this configuration for the remainder of these steps.



```
Command Result : No Error

lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: KpJ4-6YEA-SXRq-4Ebq


         Random User String: MJ3F-KAF3-CxtL-STJE

Command Result : No Error

lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo BHSM2E
BHSM2E
(kskm) root@coen:/media/HSMFD# screencap-verify
```

**Screenshot of BHSM2E STM placement during AT Ceremony 53-2 2024-03-27**

d) CA reads aloud the **Random User** string below while IW confirms that the result matches the printed screenshot from AT Ceremony 53-2 2024-03-27.
`MJ3F-KAF3-CxtL-STJE` ✓

e) Recover **BHSM2E** from STM:
`stm recover -randomuserstring MJ3F-KAF3-CxtL-STJE` ✓

**Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.**

f) IW confirms that the result matches the **Verification** string using the printed screenshot from AT Ceremony 53-2 2024-03-27.
`KpJ4-6YEA-SXRq-4Ebq` ✓

g) Once the string is verified type `proceed`, then press enter to recover **BHSM2E** from STM. ✓

</td><td>Y.Y.</td><td>18:27</td></tr>
</table>

# Register BHSM2E (Tier 7) Audit Credentials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.43 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Initialize the **audit** role: `role init -name au` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM2E touchscreen** to register a 3 of 7 **audit** credential set: ✓<br>**Note: If the BHSM2E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Auditor..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert **audit iKey 7 of 7**, then press continue. ✓<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 6<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 5<br>h) When **BHSM2E** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:28 |

## Configure BHSM2E (Tier 7) Audit Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.44 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in with the audit role:<br>`role login -name au` ✓<br>b) Follow the instructions on the **BHSM2E touchscreen** to perform **audit** authentication: ✓<br>**Note: If the BHSM2E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **audit** iKey, then press continue. 1<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 4<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 2<br>f) When **BHSM2E** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>g) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:<br>`audit time sync` ✓<br>h) Set the filepath where log files are written:<br>`audit config path /media/HSMFD/BHSM2E` ✓<br>i) Set audit logging configuration:<br>`audit config evmask all,failure,success` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Set audit logging rotation interval:<br>`audit config interval hourly@00` ✓<br>l) Set audit logging maximum log file size:<br>`audit config size 4096k` ✓<br>m) Show the audit logging configuration:<br>`audit config get` ✓<br>n) Confirm with IW the output of the logging configuration matches with the list below:<br>`Current Logging Configuration`<br>`-----------------------------`<br>`event mask          : Log everything`<br>`rotation interval : hourly@ 0 minutes past the hour`<br>`rotation size (MB) : 4`<br>`path to log         : /media/HSMFD/BHSM2E`<br>`Command Result : No Error` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:30 |

## Initialize BHSM2E (Tier 7) Administrative Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.45 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **BHSM2E** administrative partition:<br>`hsm init -label BHSM2E -iped` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM2E touchscreen** to register a 3 of 7 **SO** and 5 of 7 **domain** credential set:<br>**Note: If the BHSM2E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 3<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 4<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate **SO** authentication. 1<br>h) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue. 7<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 6<br>k) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>l) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 3<br>m) When "**Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>n) When "**Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 6<br>o) When "**Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>p) When "**Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 5<br>q) When **BHSM2E** returns to its dashboard, remove the last iKey of the **domain** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:33 |

## Configure BHSM2E (Tier 7) Global Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.46 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the **BHSM2E** admin partition slot number:<br>`slot list` ✓<br>b) Select the **BHSM2E** admin partition slot:<br>`slot set -s 105` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so` ✓<br>d) Follow the instructions on the **BHSM2E touchscreen** to perform **SO** authentication:<br>**Note: If the BHSM2E touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 5<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>h) When **BHSM2E** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, activate FIPS mode:<br>`hsm changehsmpolicy -policy 55 -value 1` ✓<br>j) Verify **BHSM2E** is in FIPS approved operation mode:<br>`hsm showinfo` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:36 |

## Back Up KSK Key Pair to BHSM2E (Tier 7) 1/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.47 | Using the **LunaCM** terminal, CA executes the following steps to perform **CO** authentication:<br>a) Verify the application partition slot number:<br>`slot list` ✓<br>b) Select the HSM's application partition slot:<br>`slot set -s 3` ✓<br>c) Log in with the Crypto Officer role:<br>`role login -name co` ✓<br>d) When **"enter password"** is displayed, enter the **secret** password:<br>`11223344` ✓<br>e) Show the KSK key pair:<br>`partition contents` ✓<br>f) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 18:37 |

## Back Up KSK Key Pair to BHSM2E (Tier 7) 2/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.48 | Using the **LunaCM** terminal, CA executes the following steps to back up KSK key pair:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initiate the backup from the HSM application partition to **BHSM2E**:<br>`partition archive backup -slot 105 -partition KSK-2024` ✓<br>b) Follow the instructions on the **BHSM2E touchscreen** to register and authenticate **SO**, Partition **SO**, **domain**, and **CO** credential sets:<br>**Note: If the BHSM2E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, begin **SO** registration by inserting a randomly selected **SO** iKey, then press continue. 4<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 6<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate Partition **SO** registration. 1<br>f) When **"Register your Partition Security Officer...** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>g) When **"Please insert first iKey"** is displayed, leave the current iKey inserted, then press continue. ✓<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 3<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate Partition **SO** authentication. 1<br>j) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>k) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>l) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 4<br>***Continued on next page*** | Y.Y. | 18:39 |

## Back Up KSK Key Pair to BHSM2E (Tier 7) 2/3 (Continued)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.49 | a) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>b) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 5<br>c) When **"Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 2<br>d) When **"Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 7<br>e) When **"Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>f) When **"Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue to automatically initiate Partition **SO** authentication. 6<br>g) When **"Please ensure an iKey is inserted"** is displayed, remove the previous iKey and insert a randomly selected **SO** iKey, then press continue. 4<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **CO** registration. 2<br>j) When **"Register your Crypto Officer"** is displayed, remove the last iKey from the previous set, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>k) When **"Please insert first iKey"** is displayed, insert a randomly selected **CO** iKey, then press continue. 3<br>l) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 2<br>m) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue to automatically initiate **CO** authentication. 6<br>n) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>o) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 7<br>p) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 3<br>q) When **BHSM2E** returns to its dashboard, remove the last iKey of the **CO** set. ✓ | Y.Y. | 18:42 |

## Back Up KSK Key Pair to BHSM2E (Tier 7) 3/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.50 | Using the **LunaCM** terminal, CA executes the following steps to verify the KSK key pair:<br>a) List the backups in **BHSM2E** by specifying **BHSM2E's** slot number:<br>`partition archive list -slot 105` ✓<br>b) List the contents of the backups in **BHSM2E**:<br>`partition archive contents -slot 105 -partition KSK-2024` ✓<br>c) Follow the instructions on the **BHSM2E touchscreen** to perform **CO** authentication:<br>**Note: If the BHSM2E touchscreen is off, tap it once to activate the display.**<br>d) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 4<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 5<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 1<br>g) When **BHSM2E** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>h) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 18:46 |

## Place BHSM2E (Tier 7) in the TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.51 | CA performs the following steps to prepare **BHSM2E** for storage:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Unplug the HSM cable from the upper USB-C port of **BHSM2E**. ✓<br>c) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below.✓<br>d) Read aloud the HSM serial number while the IW verifies it matches the information below.✓<br>e) Place the HSM into its designated new TEB, then seal it. ✓<br>f) Give IW the sealing strips for post-ceremony inventory. ✓<br>g) Place the HSM onto its designated space on the ceremony table visible to the audit camera. ✓<br>h) Initial the TEB along with IW using a ballpoint pen. ✓<br>i) Place the HSM TEB on the cart. ✓<br><br>**BHSM2E: TEB # BB02639621 / Serial # 718029** | Y.Y. | 18:47 |

✓ ✓

## BHSM1W (Tier 7) Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.52 | CA performs the following steps to prepare **BHSM1W**:<br>a) Remove the TEB from the cart and place it on the ceremony table. ✓<br>b) Inspect the TEB for tamper evidence. ✓<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>d) Remove and discard the TEB, then place **BHSM1W** on its designated stand face down to allow the audit camera to record its serial number. ✓<br>e) Read aloud the **BHSM1W** serial number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>f) Flip **BHSM1W** over face up in its designated stand. ✓<br><br>**BHSM1W: TEB # BB02638474 / Serial # 718041**<br>**Last Verified: AT Ceremony 53-2 2024-03-27** | Y.Y. | 18:49 |

## Power ON BHSM1W (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.53 | CA performs the following steps to prepare **BHSM1W**:<br>a) Plug a USB HSM cable into the USB-C port on the top of **BHSM1W**. ✓<br>b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility.<br>c) Wait for **BHSM1W** to boot and confirm the device is in Secure Transport Mode (STM). ✓<br>d) Verify the displayed HSM serial number on the screen matches **718041**. ✓<br><br>**BHSM1W: Serial # 718041** | Y.Y. | 18:50 |

# Recover BHSM1W (Tier 7) from Secure Transport Mode (STM)

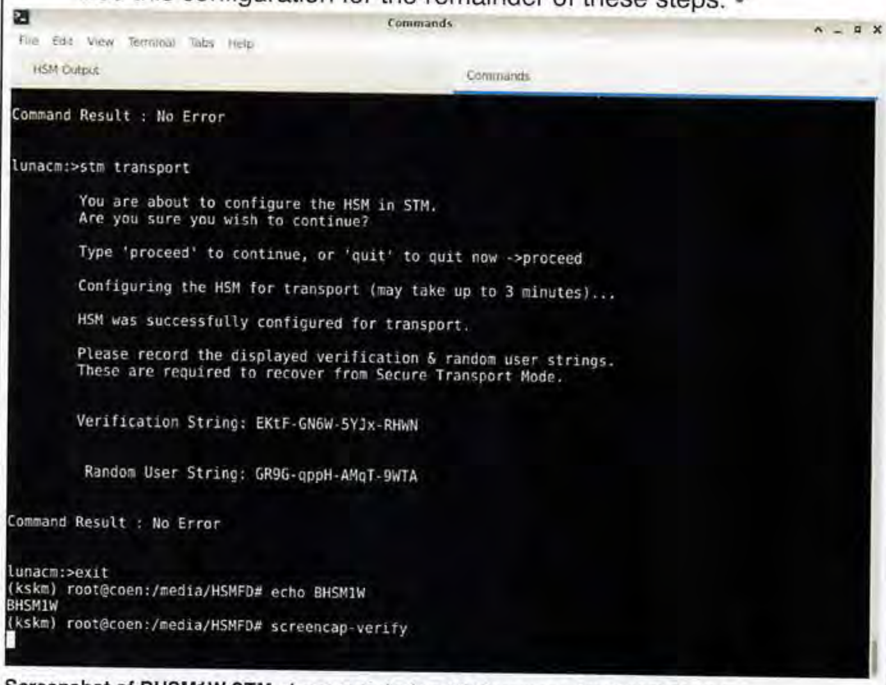
<table>
<tr><th>Step</th><th>Activity</th><th>Initials</th><th>Time</th></tr>
<tr><td>3.54</td><td>

Using the **Commands** terminal window, CA executes the following steps to recover the HSM from STM:

a) Launch the **LunaCM** application:
`lunacm` ✓

b) Select the **BHSM1W: Serial # 718041** admin partition slot:
`slot set -s 105` ✓

c) CA assigns half of the participants to confirm the strings displayed on the TV screen while the other half confirm the strings with the following image from the previous ceremony script.
Use this configuration for the remainder of these steps. ✓



```
Command Result : No Error

lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: EKtF-GN6W-5YJx-RHWN


         Random User String: GR9G-qppH-AMqT-9WTA

Command Result : No Error

lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo BHSM1W
BHSM1W
(kskm) root@coen:/media/HSMFD# screencap-verify
```

**Screenshot of BHSM1W STM placement during AT Ceremony 53-2 2024-03-27**

d) CA reads aloud the **Random User** string below while IW confirms that the result matches the printed screenshot from AT Ceremony 53-2 2024-03-27.
`GR9G-qppH-AMqT-9WTA` ✓

e) Recover **BHSM1W** from STM:
`stm recover -randomuserstring GR9G-qppH-AMqT-9WTA` ✓

**Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.**

f) IW confirms that the result matches the **Verification** string using the printed screenshot from AT Ceremony 53-2 2024-03-27.
`EKtF-GN6W-5YJx-RHWN` ✓

g) Once the string is verified type `proceed`, then press enter to recover **BHSM1W** from STM. ✓

</td><td>Y.Y.</td><td>18:54</td></tr>
</table>

## Register BHSM1W (Tier 7) Audit Credentials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.55 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Initialize the **audit** role:<br>`role init -name au` ✓<br>b) Type `proceed`, then press enter to continue.✓<br>c) Follow the instructions on the **BHSM1W touchscreen** to register a 3 of 7 **audit** credential set:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Auditor..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert a randomly selected **audit** iKey, then press continue. 1<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 2<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 3<br>h) When **BHSM1W** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:55 |

## Configure BHSM1W (Tier 7) Audit Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.56 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in with the audit role:<br>`role login -name au` ✓<br>b) Follow the instructions on the **BHSM1W touchscreen** to perform **audit** authentication:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **audit** iKey, then press continue. 4<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 5<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 7<br>f) When **BHSM1W** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>g) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:<br>`audit time sync` ✓<br>h) Set the filepath where log files are written:<br>`audit config path /media/HSMFD/BHSM1W` ✓<br>i) Set audit logging configuration:<br>`audit config evmask all,failure,success` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Set audit logging rotation interval:<br>`audit config interval hourly@00` ✓<br>l) Set audit logging maximum log file size:<br>`audit config size 4096k` ✓<br>m) Show the audit logging configuration:<br>`audit config get` ✓<br>n) Confirm with IW the output of the logging configuration matches with the list below:<br><br>`Current Logging Configuration`<br>`-----------------------------`<br>`event mask         : Log everything`<br>`rotation interval : hourly@ 0 minutes past the hour`<br>`rotation size (MB) : 4`<br>`path to log        : /media/HSMFD/BHSM1W`<br><br>`Command Result : No Error`<br><br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 18:57 |

# Initialize BHSM1W (Tier 7) Administrative Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.57 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **BHSM1W** administrative partition: `hsm init -label BHSM1W -iped` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM1W touchscreen** to register a 3 of 7 **SO** and 5 of 7 **domain** credential set:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 1<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 6<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate **SO** authentication. 2<br>h) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue. ~~8~~ 3<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 4<br>k) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>l) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 2<br>m) When "**Please insert iKey 2 of 5**" is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>n) When "**Please insert iKey 3 of 5**" is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 6<br>o) When "**Please insert iKey 4 of 5**" is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 7<br>p) When "**Please insert iKey 5 of 5**" is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 5<br>q) When **BHSM1W** returns to its dashboard, remove the last iKey of the **domain** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:00 |

## Configure BHSM1W (Tier 7) Global Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.58 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the **BHSM1W** admin partition slot number:<br>`slot list` ✓<br>b) Select the **BHSM1W** admin partition slot:<br>`slot set -s 105` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so`✓<br>d) Follow the instructions on the **BHSM1W touchscreen** to perform **SO** authentication:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue.✓3<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 4<br>h) When **BHSM1W** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, activate FIPS mode:<br>`hsm changehsmpolicy -policy 55 -value 1` ✓<br>j) Verify **BHSM1W** is in FIPS approved operation mode:<br>`hsm showinfo`✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:01 |

## Back Up KSK Key Pair to BHSM1W (Tier 7) 1/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.59 | Using the **LunaCM** terminal, CA executes the following steps to perform **CO** authentication:<br>a) Verify the application partition slot number:<br>`slot list` ✓<br>b) Select the HSM's application partition slot:<br>`slot set -s 3`✓<br>c) Log in with the Crypto Officer role:<br>`role login -name co` ✓<br>d) When **"enter password"** is displayed, enter the **secret** password:<br>`11223344` ✓<br>e) Show the KSK key pair:<br>`partition contents` ✓<br>f) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 19:02 |

# Back Up KSK Key Pair to BHSM1W (Tier 7) 2/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.60 | Using the **LunaCM** terminal, CA executes the following steps to back up KSK key pair:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initiate the backup from the HSM application partition to **BHSM1W**:<br>`partition archive backup -slot 105 -partition KSK-2024` ✓<br>b) Follow the instructions on the **BHSM1W touchscreen** to register and authenticate **SO**, Partition **SO**, **domain**, and **CO** credential sets:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, begin **SO** registration by inserting a randomly selected **SO** iKey, then press continue. 3<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate Partition **SO** registration. 2<br>f) When **"Register your Partition Security Officer...** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>g) When **"Please insert first iKey"** is displayed, leave the current iKey inserted, then press continue. ✓<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate Partition **SO** authentication. 4<br>j) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>k) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>l) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 3<br>***Continued on next page*** | Y.Y. | 19:04 |

## Back Up KSK Key Pair to BHSM1W (Tier 7) 2/3 (Continued)

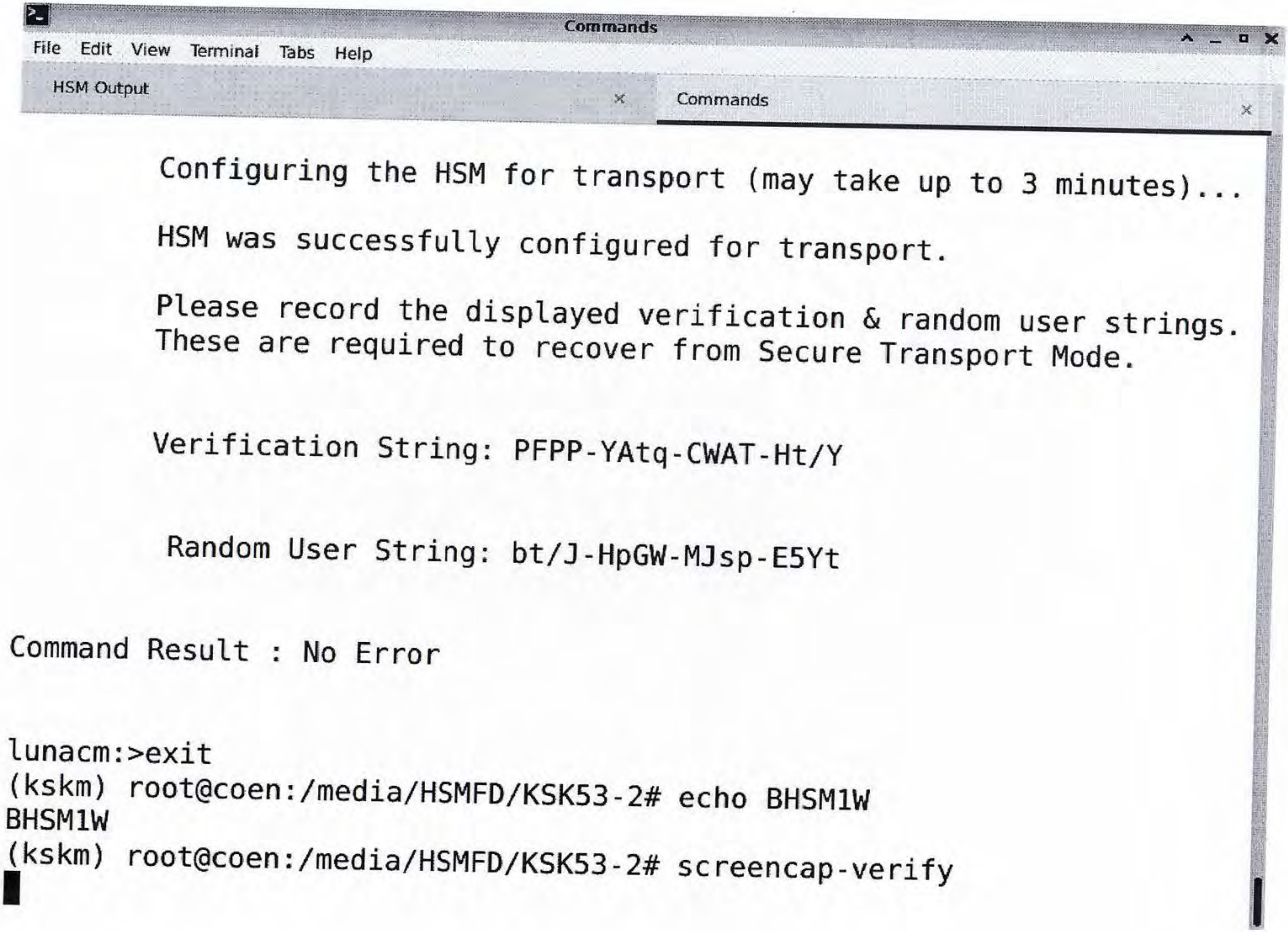
| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.61 | a) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>b) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 6<br>c) When **"Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 5<br>d) When **"Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>e) When **"Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 7<br>f) When **"Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue to automatically initiate Partition **SO** authentication. 2<br>g) When **"Please ensure an iKey is inserted"** is displayed, remove the previous iKey and insert a randomly selected **SO** iKey, then press continue. 5<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 6<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **CO** registration. 2<br>j) When **"Register your Crypto Officer"** is displayed, remove the last iKey from the previous set, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>k) When **"Please insert first iKey"** is displayed, insert a randomly selected **CO** iKey, then press continue. 4<br>l) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 5<br>m) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue to automatically initiate **CO** authentication. 3<br>n) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>o) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 1<br>p) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 7<br>q) When **BHSM1W** returns to its dashboard, remove the last iKey of the **CO** set. ✓ | Y.Y. | 19:07 |

## Back Up KSK Key Pair to BHSM1W (Tier 7) 3/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.62 | Using the **LunaCM** terminal, CA executes the following steps to verify the KSK key pair:<br>a) List the backups in **BHSM1W** by specifying **BHSM1W's** slot number:<br>`partition archive list -slot 105` ✓<br>b) List the contents of the backups in **BHSM1W**:<br>`partition archive contents -slot 105 -partition KSK-2024` ✓<br>c) Follow the instructions on the **BHSM1W touchscreen** to perform **CO** authentication:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>d) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 2<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 4<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 6<br>g) When **BHSM1W** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>h) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 19:09 |

## Place BHSM1W (Tier 7) into Secure Transport Mode (STM)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.63 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the admin partition slot number:<br>`slot list` ✓<br>b) Select the **BHSM1W** application partition slot:<br>`slot set -s 105` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so` ✓<br>d) Follow the instructions on the **BHSM1W touchscreen** to perform **SO** authentication:<br>**Note: If the BHSM1W touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 5<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>h) When **BHSM1W** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, place **BHSM1W** into STM:<br>`stm transport` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Verify the **BHSM1W** dashboard indicates the device is in **Secure Transport Mode** and the random and verification strings are displayed in the terminal window. ✓ | Y.Y. | 19:13 |



```
        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: PFPP-YAtq-CWAT-Ht/Y


         Random User String: bt/J-HpGW-MJsp-E5Yt


Command Result : No Error


lunacm:>exit
(kskm) root@coen:/media/HSMFD/KSK53-2# echo BHSM1W
BHSM1W
(kskm) root@coen:/media/HSMFD/KSK53-2# screencap-verify
█
```

## Print BHSM1W Secure Transport Mode (STM) Strings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.64 | CA executes the following steps:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Using the **Commands** terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot):<br>`echo BHSM1W` ✓<br>c) Print two copies of the STM strings, then verify the screenshot:<br>`screencap-verify` ✓<br>**Note: One copy for the audit bundle and one copy for the BHSM1W TEB.** ✓<br>d) Upon successful verification of the screenshot, close the image viewer application. ✓ | Y.Y. | 19:15 |

## Place BHSM1W (Tier 7) in the TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.65 | CA performs the following steps to prepare **BHSM1W** for storage:<br>a) Unplug the HSM cable from the upper USB-C port of **BHSM1W**. ✓<br>b) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>c) Read aloud the HSM serial number while the IW verifies it matches the information below. ✓<br>d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. ✓<br>e) Give IW the sealing strips for post-ceremony inventory. ✓<br>f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. ✓<br>g) Initial the TEB along with IW using a ballpoint pen. ✓<br>h) Call RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. ✓<br>i) Give RKOS the TEB. ✓<br><br>**BHSM1W: TEB # BB02639620 ✓ / Serial # 718041 ✓** | Y.Y. | 19:17 |

## BHSM2W (Tier 7) Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.66 | CA performs the following steps to prepare **BHSM2W**:<br>a) Remove the TEB from the cart and place it on the ceremony table. ✓<br>b) Inspect the TEB for tamper evidence. ✓<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>d) Remove and discard the TEB, then place **BHSM2W** on its designated stand face down to allow the audit camera to record its serial number. ✓<br>e) Read aloud the **BHSM2W** serial number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>f) Flip **BHSM2W** over face up in its designated stand. ✓<br><br>**BHSM2W: TEB # BB02638473 / Serial # 718018**<br>**Last Verified: AT Ceremony 53-2 2024-03-27** | Y.Y. | 19:19. |

## Power ON BHSM2W (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| **3.67** | CA performs the following steps to prepare **BHSM2W**:<br>a) Plug a USB HSM cable into the USB-C port on the top of **BHSM2W**. ✓<br>b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. ✓<br>c) Wait for **BHSM2W** to boot and confirm the device is in Secure Transport Mode (STM). ✓<br>d) Verify the displayed HSM serial number on the screen matches **718018**. ✓<br>**BHSM2W: Serial # 718018** | Y.Y. | 19:22 |

## Recover BHSM2W (Tier 7) from Secure Transport Mode (STM)

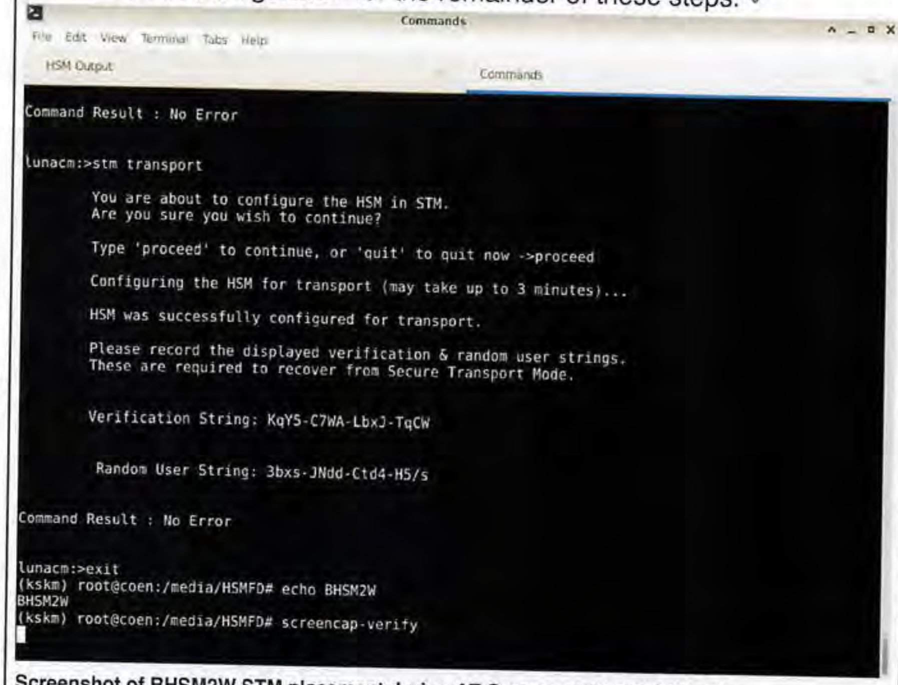
<table>
<tr><th>Step</th><th>Activity</th><th>Initials</th><th>Time</th></tr>
<tr><td>3.68</td><td>

Using the **Commands** terminal window, CA executes the following steps to recover the HSM from STM:

a) Launch the **LunaCM** application:
`lunacm` ✓

b) Select the **BHSM2W: Serial # 718018** admin partition slot:
`slot set -s 105` ✓

c) CA assigns half of the participants to confirm the strings displayed on the TV screen while the other half confirm the strings with the following image from the previous ceremony script.
Use this configuration for the remainder of these steps. ✓



```
Command Result : No Error

lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: KqY5-C7WA-LbxJ-TqCW


         Random User String: 3bxs-JNdd-Ctd4-H5/s

Command Result : No Error

lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo BHSM2W
BHSM2W
(kskm) root@coen:/media/HSMFD# screencap-verify
```

**Screenshot of BHSM2W STM placement during AT Ceremony 53-2 2024-03-27**

d) CA reads aloud the **Random User** string below while IW confirms that the result matches the printed screenshot from AT Ceremony 53-2 2024-03-27.
`3bxs-JNdd-Ctd4-H5/s` ✓

e) Recover **BHSM2W** from STM:
`stm recover -randomuserstring 3bxs-JNdd-Ctd4-H5/s` ✓

**Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.**

f) IW confirms that the result matches the **Verification** string using the printed screenshot from AT Ceremony 53-2 2024-03-27.
`KqY5-C7WA-LbxJ-TqCW` ✓

g) Once the string is verified type `proceed`, then press enter to recover **BHSM2W** from STM. ✓

</td><td>Y.Y.</td><td>19:27</td></tr>
</table>

## Register BHSM2W (Tier 7) Audit Credentials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.69 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Initialize the **audit** role:<br>`role init -name au` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM2W touchscreen** to register a 3 of 7 **audit** credential set:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Auditor..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue.✓<br>e) When **"Please insert first iKey"** is displayed, insert a randomly selected **audit** iKey, then press continue. 3<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 2<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 6<br>h) When **BHSM2W** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:28 |

## Configure BHSM2W (Tier 7) Audit Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.70 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in with the audit role:<br>`role login -name au` ✓<br>b) Follow the instructions on the **BHSM2W touchscreen** to perform **audit** authentication:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **audit** iKey, then press continue. ✓ 4<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 5<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 7<br>f) When **BHSM2W** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>g) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:<br>`audit time sync` ✓<br>h) Set the filepath where log files are written:<br>`audit config path /media/HSMFD/BHSM2W` ✓<br>i) Set audit logging configuration:<br>`audit config evmask all,failure,success` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Set audit logging rotation interval:<br>`audit config interval hourly@00` ✓<br>l) Set audit logging maximum log file size:<br>`audit config size 4096k` ✓<br>m) Show the audit logging configuration:<br>`audit config get` ✓<br>n) Confirm with IW the output of the logging configuration matches with the list below:<br><br>`Current Logging Configuration`<br>`-----------------------------`<br>`event mask        : Log everything`<br>`rotation interval : hourly@ 0 minutes past the hour`<br>`rotation size (MB): 4`<br>`path to log       : /media/HSMFD/BHSM2W`<br><br>`Command Result : No Error`<br><br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:30 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 3 Step(s): 71-e Page(s): 63<br>Date and time of the exception: 2024/04/26 @ 19:35<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 19:35 |

CA accidentally inserted CO key instead of SO key. We got out of error screen, and successfuly continued

## Initialize BHSM2W (Tier 7) Administrative Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.71 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **BHSM2W** administrative partition: `hsm init -label BHSM2W -iped` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **BHSM2W touchscreen** to register a 3 of 7 **SO** and 5 of 7 **domain** credential set:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>* e) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 6<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate **SO** authentication. 7<br>h) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue. 4<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 1<br>k) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>l) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 2<br>m) When "**Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>n) When "**Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 6<br>o) When "**Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>p) When "**Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 7<br>q) When **BHSM2W** returns to its dashboard, remove the last iKey of the **domain** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:36 |

## Configure BHSM2W (Tier 7) Global Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.72 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the **BHSM2W** admin partition slot number:<br>`slot list` ✓<br>b) Select the **BHSM2W** admin partition slot:<br>`slot set -s 105` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so` ✓<br>d) Follow the instructions on the **BHSM2W touchscreen** to perform **SO** authentication:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 3<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>h) When **BHSM2W** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, activate FIPS mode:<br>`hsm changehsmpolicy -policy 55 -value 1` ✓<br>j) Verify **BHSM2W** is in FIPS approved operation mode:<br>`hsm showinfo` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:37 |

## Back Up KSK Key Pair to BHSM2W (Tier 7) 1/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.73 | Using the **LunaCM** terminal, CA executes the following steps to perform **CO** authentication:<br>a) Verify the application partition slot number:<br>`slot list` ✓<br>b) Select the HSM's application partition slot:<br>`slot set -s 3` ✓<br>c) Log in with the Crypto Officer role:<br>`role login -name co` ✓<br>d) When **"enter password"** is displayed, enter the **secret** password:<br>`11223344` ✓<br>e) Show the KSK key pair: ✓<br>`partition contents`<br>f) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 19:38 |

## Back Up KSK Key Pair to BHSM2W (Tier 7) 2/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.74 | Using the **LunaCM** terminal, CA executes the following steps to back up KSK key pair:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initiate the backup from the HSM application partition to **BHSM2W**:<br>`partition archive backup -slot 105 -partition KSK-2024` ✓<br>b) Follow the instructions on the **BHSM2W touchscreen** to register and authenticate **SO**, Partition **SO**, **domain**, and **CO** credential sets:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, begin **SO** registration by inserting a randomly selected **SO** iKey, then press continue. 7<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 10<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate Partition **SO** registration. 4<br>f) When **"Register your Partition Security Officer...** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>g) When **"Please insert first iKey"** is displayed, leave the current iKey inserted, then press continue. ✓<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate Partition **SO** authentication. 1<br>j) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>k) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>l) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 4<br>*Continued on next page* | Y.Y. | 19:40 |

## Back Up KSK Key Pair to BHSM2W (Tier 7) 2/3 (Continued)

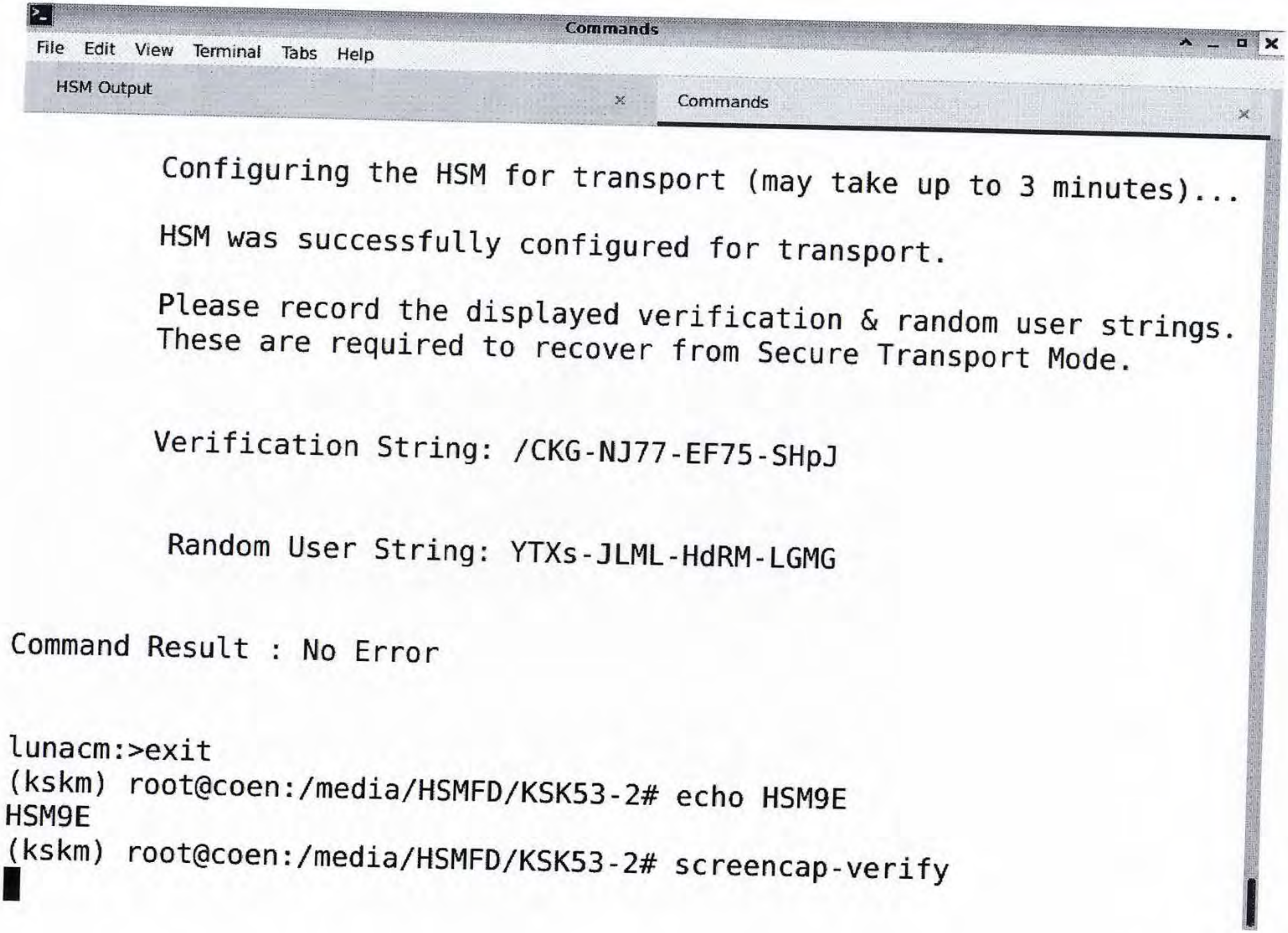
| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.75 | a) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>b) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 3<br>c) When **"Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>d) When **"Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 6<br>e) When **"Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>f) When **"Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue to automatically initiate Partition **SO** authentication. 7<br>g) When **"Please ensure an iKey is inserted"** is displayed, remove the previous iKey and insert a randomly selected **SO** iKey, then press continue. 4<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **CO** registration. 7<br>j) When **"Register your Crypto Officer"** is displayed, remove the last iKey from the previous set, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>k) When **"Please insert first iKey"** is displayed, insert a randomly selected **CO** iKey, then press continue. 3<br>l) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 5<br>m) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue to automatically initiate **CO** authentication. 2<br>n) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>o) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 4<br>p) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 1<br>q) When **BHSM2W** returns to its dashboard, remove the last iKey of the **CO** set. ✓ | Y.Y. | 19:43 |

## Back Up KSK Key Pair to BHSM2W (Tier 7) 3/3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.76 | Using the **LunaCM** terminal, CA executes the following steps to verify the KSK key pair:<br>a) List the backups in **BHSM2W** by specifying **BHSM2W's** slot number:<br>`partition archive list -slot 105` ✓<br>b) List the contents of the backups in **BHSM2W**:<br>`partition archive contents -slot 105 -partition KSK-2024` ✓<br>c) Follow the instructions on the **BHSM2W touchscreen** to perform **CO** authentication:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>d) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 5<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 6<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 7<br>g) When **BHSM2W** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>h) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 19:44 |

## Place HSM9E (Tier 7) into Secure Transport Mode (STM)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.77 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the admin partition slot number:<br>`slot list` ✓<br>b) Select the **HSM9E** application partition slot:<br>`slot set -s 3` ✓<br>c) Deactivate the **CO** role:<br>`role deactivate -name co` ✓<br>d) Select the **HSM9E** admin partition slot:<br>`slot set -s 4` ✓<br>e) Log in with the Security Officer role:<br>`role login -name so` ✓<br>f) Follow the instructions on the **HSM9E touchscreen** to perform **SO** authentication:<br>**Note: If the HSM9E touchscreen is off, tap it once to activate the display.**<br>g) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 2<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>j) When **HSM9E** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>k) Using the **LunaCM** terminal, place **HSM9E** into STM:<br>`stm transport` ✓<br>l) Type `proceed`, then press enter to continue. ✓<br>m) Verify the **HSM9E** dashboard indicates the device is in **Secure Transport Mode** and the random and verification strings are displayed in the terminal window. ✓ | Y.Y. | 19:48 |



```
        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: /CKG-NJ77-EF75-SHpJ


         Random User String: YTXs-JLML-HdRM-LGMG


Command Result : No Error


lunacm:>exit
(kskm) root@coen:/media/HSMFD/KSK53-2# echo HSM9E
HSM9E
(kskm) root@coen:/media/HSMFD/KSK53-2# screencap-verify
█
```

## Print HSM9E Secure Transport Mode (STM) Strings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.78 | CA executes the following steps:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Using the **Commands** terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot):<br>`echo HSM9E` ✓<br>c) Print two copies of the STM strings, then verify the screenshot:<br>`screencap-verify` ✓<br>**Note: One copy for the audit bundle and one copy for the HSM9E TEB.**<br>d) Upon successful verification of the screenshot, close the image viewer application. ✓ | Y.Y. | 19:49 |

## Place HSM9E (Tier 7) in the TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.79 | CA performs the following steps to prepare **HSM9E** for storage:<br>a) Unplug the HSM cable from the upper USB-C port of **HSM9E**. ✓<br>b) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>c) Read aloud the HSM serial number while the IW verifies it matches the information below. ✓<br>d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. ✓<br>e) Give IW the sealing strips for post-ceremony inventory. ✓<br>f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. ✓<br>g) Initial the TEB along with IW using a ballpoint pen. ✓<br>h) Place the HSM TEB on the cart. ✓<br><br>**HSM9E: TEB # BB02639624 / Serial # 712482** | Y.Y. | 19:50 |

## HSM10E (Tier 7) Setup

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.80 | CA performs the following steps to prepare **HSM10E**:<br>a) Remove the TEB from the cart and place it on the ceremony table. ✓<br>b) Inspect the TEB for tamper evidence. ✓<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>d) Remove and discard the TEB, then place **HSM10E** on its designated stand face down to allow the audit camera to record its serial number. ✓<br>e) Read aloud the **HSM10E** serial number while IW verifies the information using the previous ceremony script where it was last used. ✓<br>f) Flip **HSM10E** over face up in its designated stand. ✓<br><br>**HSM10E: TEB # BB02638472 / Serial # 712477**<br>**Last Verified: AT Ceremony 53-2 2024-03-27** | Y.Y. | 19:52 |

## Power ON HSM10E (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.81 | CA performs the following steps to prepare **HSM10E**:<br>a) Plug a USB HSM cable into the USB-C port on the top of **HSM10E**. ✓<br>b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. ✓<br>c) Wait for **HSM10E** to boot and confirm the device is in Secure Transport Mode (STM). ✓<br>d) Verify the displayed HSM serial number on the screen matches **712477**. ✓<br>**HSM10E: Serial # 712477** | Y.Y. | 19:54 |

## Recover HSM10E (Tier 7) from Secure Transport Mode (STM)

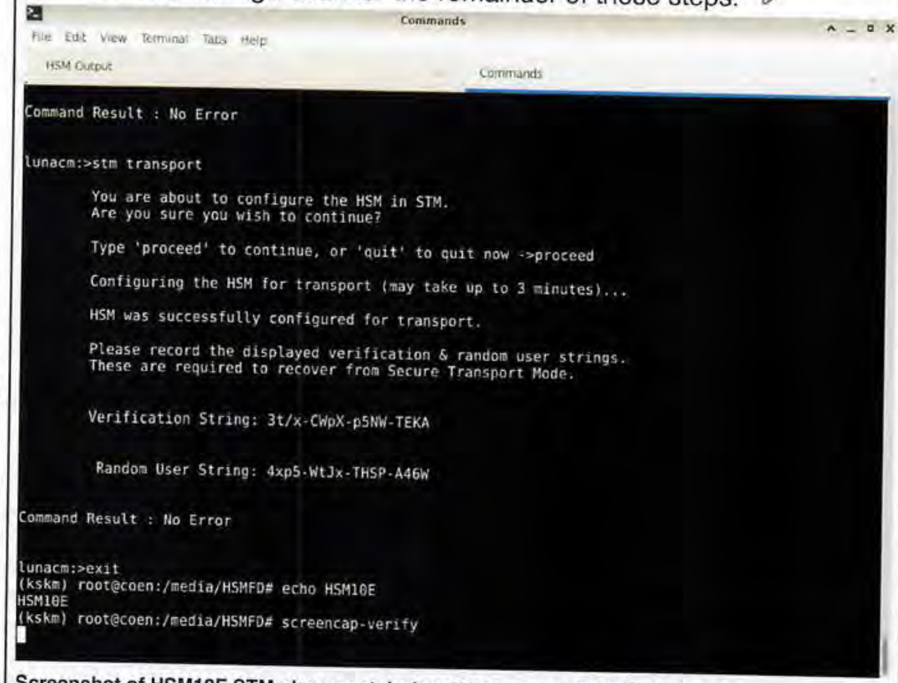
<table>
<tr><th>Step</th><th>Activity</th><th>Initials</th><th>Time</th></tr>
<tr><td>3.82</td><td>

Using the **Commands** terminal window, CA executes the following steps to recover the HSM from STM:

a) Launch the **LunaCM** application:
`lunacm` ✓

b) Select the **HSM10E: Serial # 712477** admin partition slot:
`slot set -s 4` ✓

c) CA assigns half of the participants to confirm the strings displayed on the TV screen while the other half confirm the strings with the following image from the previous ceremony script.
Use this configuration for the remainder of these steps. ✓



```
Command Result : No Error


lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: 3t/x-CWpX-p5NW-TEKA


         Random User String: 4xp5-WtJx-THSP-A46W

Command Result : No Error


lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo HSM10E
HSM10E
(kskm) root@coen:/media/HSMFD# screencap-verify
```

**Screenshot of HSM10E STM placement during AT Ceremony 53-2 2024-03-27**

d) CA reads aloud the **Random User** string below while IW confirms that the result matches the printed screenshot from AT Ceremony 53-2 2024-03-27.
`4xp5-WtJx-THSP-A46W` ✓

e) Recover **HSM10E** from STM:
`stm recover -randomuserstring 4xp5-WtJx-THSP-A46W` ✓

**Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.**

f) IW confirms that the result matches the **Verification** string using the printed screenshot from AT Ceremony 53-2 2024-03-27.
`3t/x-CWpX-p5NW-TEKA` ✓

g) Once the string is verified type `proceed`, then press enter to recover **HSM10E** from STM. ✓

</td><td>Y.Y.</td><td>19:57</td></tr>
</table>

## Register HSM10E (Tier 7) Audit Credentials

| Step | Activity | Initials | Time |
|---|---|---|---|
| **3.83** | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Initialize the **audit** role:<br>`role init -name au` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **HSM10E touchscreen** to register a 3 of 7 **audit** credential set:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Auditor..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert a randomly selected **audit** iKey, then press continue. 3<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 1<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 4<br>h) When **HSM10E** returns to its dashboard, remove the last iKey of the **audit** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 19:58 |

# Configure HSM10E (Tier 7) Audit Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.84 |  | Y.Y. | 20:00 |

Using the **LunaCM** terminal, CA executes the following steps:

a) Log in with the audit role:

```
role login -name au
```
✓

b) Follow the instructions on the **HSM10E touchscreen** to perform **audit** authentication:

**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**

c) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **audit** iKey, then press continue. 5

d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 7

e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. 6

f) When **HSM10E** returns to its dashboard, remove the last iKey of the **audit** set. ✓

g) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:

```
audit time sync
```
✓

h) Set the filepath where log files are written:

```
audit config path /media/HSMFD/HSM10E
```
✓

i) Set audit logging configuration:

```
audit config evmask all,failure,success
```
✓

j) Type `proceed`, then press enter to continue. ✓

k) Set audit logging rotation interval:

```
audit config interval hourly@00
```
✓

l) Set audit logging maximum log file size:

```
audit config size 4096k
```
✓

m) Show the audit logging configuration:

```
audit config get
```
✓

n) Confirm with IW the output of the logging configuration matches with the list below:

```
Current Logging Configuration
-----------------------------
event mask          : Log everything
rotation interval : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log         : /media/HSMFD/HSM10E

Command Result : No Error
```

**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.**

## Initialize HSM10E (Tier 7) Administrative Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.85 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **HSM10E** administrative partition: `hsm init -label HSM10E -iped` ✓<br>b) Type `proceed`, then press enter to continue. ✓<br>c) Follow the instructions on the **HSM10E touchscreen** to register a 3 of 7 **SO** and 5 of 7 **domain** credential set:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>d) When **"Register your Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>e) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 5<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 4<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate **SO** authentication. 1<br>h) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue. 7<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 2<br>k) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>l) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 6<br>m) When "**Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 2<br>n) When "**Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>o) When "**Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 5<br>p) When "**Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 7<br>q) When **HSM10E** returns to its dashboard, remove the last iKey of the **domain** set. ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 20:03 |

## Configure HSM10E (Tier 7) Global Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.86 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the **HSM10E** admin partition slot number:<br>`slot list` ✓<br>b) Select the **HSM10E** admin partition slot:<br>`slot set -s 4` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so` ✓<br>d) Follow the instructions on the **HSM10E touchscreen** to perform **SO** authentication:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 4<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 3<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>h) When **HSM10E** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, activate FIPS mode:<br>`hsm changeHP -policy 12 -value 0` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Disable PIN change after setup:<br>`hsm changeHP -policy 21 -value 0` ✓<br>l) Verify **HSM10E** is in FIPS approved operation mode:<br>`hsm showinfo` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 20:06 |

## Create HSM10E (Tier 7) Application Partition

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.87 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Create the partition:<br>`partition create` ✓<br>b) Verify the application partition slot number:<br>`slot list` ✓<br>c) Select the application partition slot:<br>`slot set -s 3` ✓<br>d) Initialize the application partition:<br>`partition init -label HSM10E_KSK-2024` ✓<br>e) Type `proceed`, then press enter to continue. ✓<br>f) Follow the instructions on the **HSM10E touchscreen** to register the **SO** and **domain** credential sets:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>g) When **"Register your Partition Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>h) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. ✓ 1<br>i) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 2<br>j) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate Partition **SO** authentication. 6<br>k) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. ✓<br>l) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 5<br>m) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. 7<br>n) When **"Set up your domain..."** is displayed, remove the last iKey from the previous set, select **"Join existing domain"**, then press continue. ✓<br>o) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. 5<br>p) When **"Please insert iKey 2 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 1<br>q) When **"Please insert iKey 3 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 7<br>r) When **"Please insert iKey 4 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 2<br>s) When **"Please insert iKey 5 of 5"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. 4<br>t) When **HSM10E** returns to its dashboard, remove the last iKey of the **domain** set. ✓<br>**Note 1: The "KE-CL" displayed on the dashboard indicates Key Export and Cloning are enabled.**<br>**Note 2: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 20:10 |

## Configure HSM10E (Tier 7) Partition Policies

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.88 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Log in as the Partition Officer:<br>`role login -name po` ✓<br>b) Follow the instructions on the **HSM10E touchscreen** to perform Partition **SO** authentication:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. 4<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 7<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>f) When **HSM10E** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>g) Using the **LunaCM** terminal, allow partition activation with PIN:<br>`partition changepolicy -policy 22 -value 1` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 20:11 |

## Register HSM10E (Tier 7) CO Credentials and PIN

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.89 | Using the **LunaCM** terminal, CA executes the following steps:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Initialize the **CO** role:<br>`role init -name co` ✓<br>b) Follow the instructions on the **HSM10E touchscreen** to register a 3 of 7 **CO** credential set:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>c) When **"Register your Crypto Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. ✓<br>d) When **"Please insert first iKey"** is displayed, insert a randomly selected **CO** iKey, then press continue. 2<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 4<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 5<br>g) When **HSM10E** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>h) Using the **LunaCM** terminal, configure a **CO** PIN:<br>`role createchallenge -name co` ✓<br>i) When **"Enter new challenge secret:"** is displayed, type `11223344`, then press enter. ✓<br>j) When **"Re-enter new challenge secret:"** is displayed, type `11223344`, then press enter. ✓<br>k) Log out of **CO** role: ✓<br>`role logout` ✓<br>**Note: Use the iKey credentials hanging furthest out on each respective hook of the credential stand as required. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 94.** | Y.Y. | 20:13 |

## Restore the KSK Key Pair to HSM10E (Tier 7)

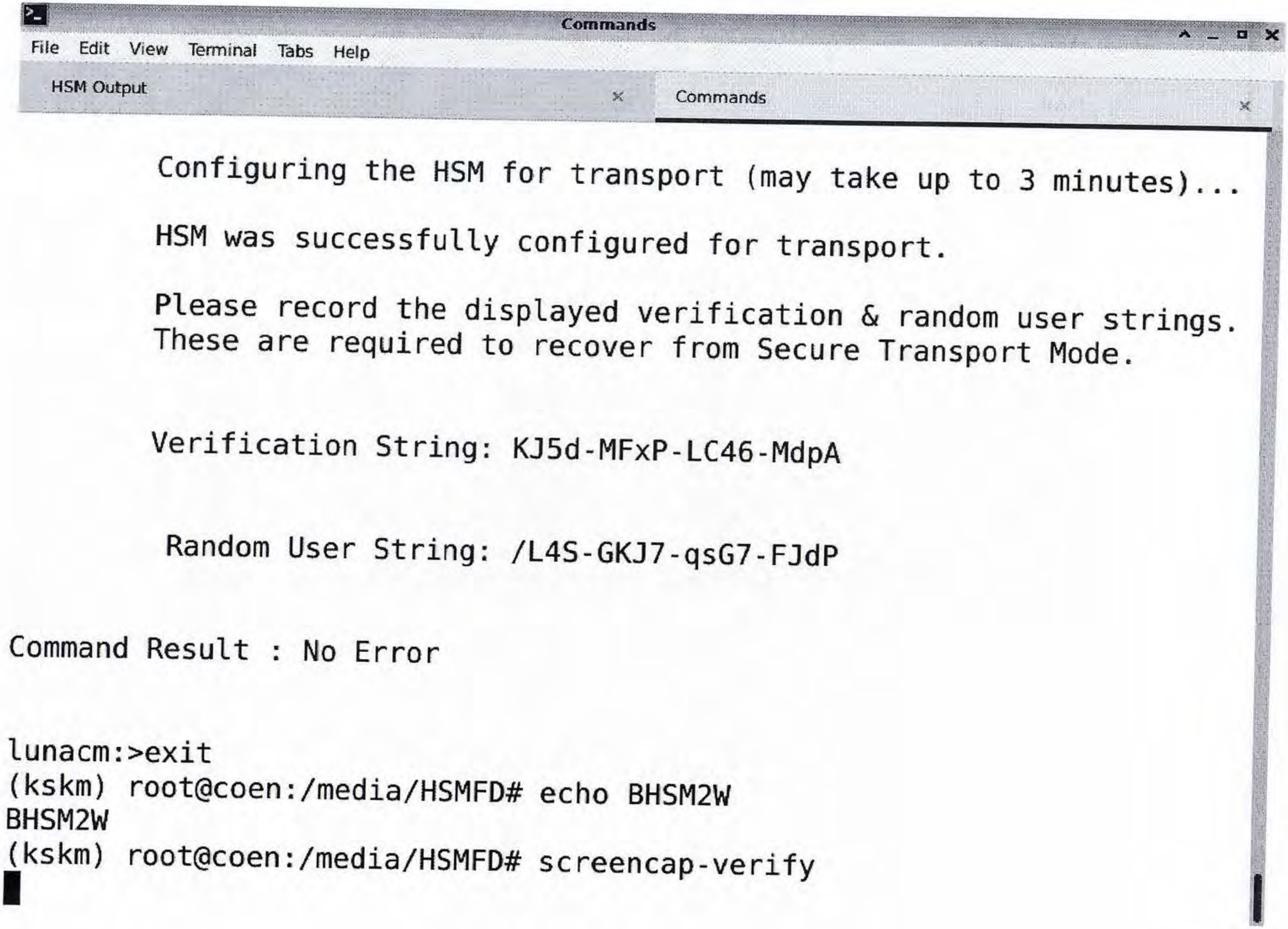
| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.90 | Using the **LunaCM** terminal, CA executes the following steps to restore the KSK key pair:<br>**Note: The CA may delegate narration of this step to the MC to aid concentration. Questions should be held until PED sequences finish to avoid timeout.**<br>a) Log in with the Crypto Officer role:<br>`role login -name co` ✓<br>b) When **"enter password"** is displayed, enter the **secret** password:<br>`11223344` ✓<br>c) Follow the instructions on the **HSM10E touchscreen** to perform **CO** authentication:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>d) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 3<br>e) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 4<br>f) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 7<br>g) When **HSM10E** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>h) Verify the **BHSM2W** admin partition slot number:<br>`slot list` ✓<br>i) List the backups in **BHSM2W** by specifying **BHSM2W's** slot number:<br>`partition archive list -slot 105` ✓<br>j) List the content of the backups in **BHSM2W**:<br>`partition archive contents -slot 105 -partition KSK-2024` ✓<br>k) Follow the instructions on the **BHSM2W touchscreen** to perform **CO** authentication:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>l) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 7<br>m) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 2<br>n) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 5<br>o) When **BHSM2W** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br><br>***Continued on next page*** | Y.Y. | 20:16 |

## Restore the KSK Key Pair to HSM10E (Tier 7) (Continued)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.91 | Using the **LunaCM** terminal, CA executes the following steps to restore the KSK key pair:<br>a) Initiate the restore from **BHSM2W** to **HSM10E**:<br>`partition archive restore -slot 105 -partition KSK-2024` ✓<br>b) Follow the instructions on the **BHSM2W touchscreen** to perform **CO** authentication:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>c) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue. 2<br>d) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 1<br>e) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue. 4<br>f) When **BHSM2W** returns to its dashboard, remove the last iKey of the **CO** set. ✓<br>g) Display the KSK key pair on **HSM10E**:<br>`partition contents` ✓<br>h) Match the displayed KSK label with the key label indicated on step **3.27** ✓ | Y.Y. | 20:18 |

## Verify KSK Key Pair in HSM10E (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.92 | Using the **LunaCM, then Commands** terminal, CA executes the following steps to verify the KSK key pair:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Using the **Commands** terminal window, verify the presence of the keypair created previously:<br>`kskm-keymaster --hsm luna inventory` ✓<br>c) Match the displayed KSK label with the key label indicated on step **3.27** ✓<br>d) Execute the command below to change the working directory:<br>`cd /media/HSMFD` ✓<br>e) launch **LunaCM**:<br>`lunacm` ✓ | Y.Y. | 20:23 |



```
        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: KJ5d-MFxP-LC46-MdpA


         Random User String: /L4S-GKJ7-qsG7-FJdP


Command Result : No Error


lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo BHSM2W
BHSM2W
(kskm) root@coen:/media/HSMFD# screencap-verify
█
```

## Place BHSM2W (Tier 7) into Secure Transport Mode (STM)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.93 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the admin partition slot number:<br>`slot list` ✓<br>b) Select the **BHSM2W** application partition slot:<br>`slot set -s 105` ✓<br>c) Log in with the Security Officer role:<br>`role login -name so` ✓<br>d) Follow the instructions on the **BHSM2W touchscreen** to perform **SO** authentication:<br>**Note: If the BHSM2W touchscreen is off, tap it once to activate the display.**<br>e) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 5<br>f) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 6<br>g) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 1<br>h) When **BHSM2W** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>i) Using the **LunaCM** terminal, place **BHSM2W** into STM:<br>`stm transport` ✓<br>j) Type `proceed`, then press enter to continue. ✓<br>k) Verify the **BHSM2W** dashboard indicates the device is in **Secure Transport Mode** and the random and verification strings are displayed in the terminal window. ✓ | Y.Y. | 20:27 |

## Print BHSM2W Secure Transport Mode (STM) Strings

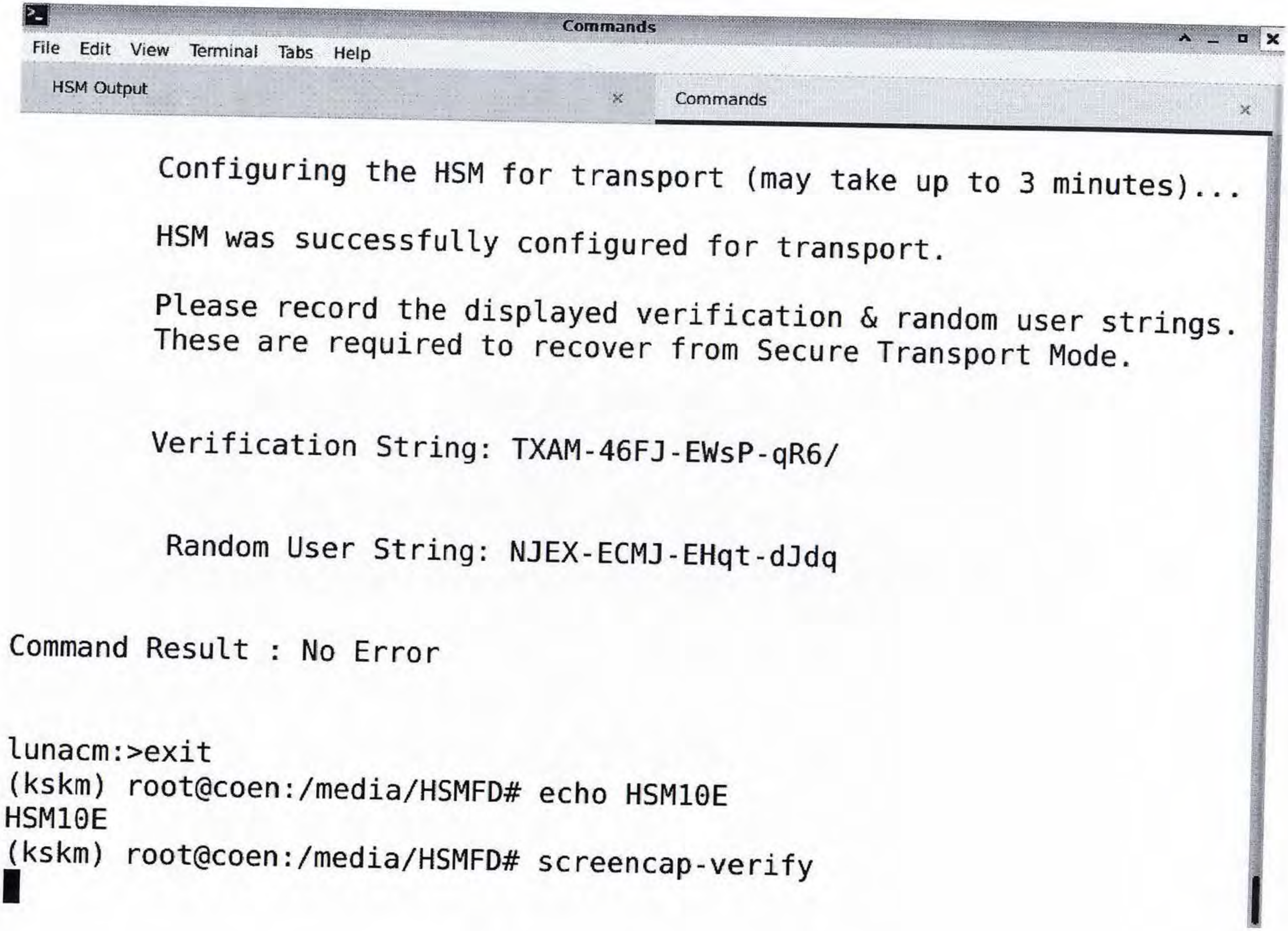
| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.94 | CA executes the following steps:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Using the **Commands** terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot):<br>`echo BHSM2W` ✓<br>c) Print two copies of the STM strings, then verify the screenshot:<br>`screencap-verify` ✓<br>**Note: One copy for the audit bundle and one copy for the BHSM2W TEB.**<br>d) Upon successful verification of the screenshot, close the image viewer application. ✓ | Y.Y. | 20:27 |

## Place BHSM2W (Tier 7) in the TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.95 | CA performs the following steps to prepare **BHSM2W** for storage:<br>a) Unplug the HSM cable from the upper USB-C port of **BHSM2W**. ✓<br>b) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>c) Read aloud the HSM serial number while the IW verifies it matches the information below. ✓<br>d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. ✓<br>e) Give IW the sealing strips for post-ceremony inventory. ✓<br>f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. ✓<br>g) Initial the TEB along with IW using a ballpoint pen. ✓<br>h) Call RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. ✓<br>i) Give RKOS the TEB. ✓<br><br>**BHSM2W: TEB # BB02639619 ✓ / Serial # 718018 ✓** | Y.Y. | 20:29 |

## Launch LunaCM

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.96 | CA executes the following steps to launch **LunaCM**:<br>`lunacm` ✓ | Y.Y. | 20:30 |



```
        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: TXAM-46FJ-EWsP-qR6/


         Random User String: NJEX-ECMJ-EHqt-dJdq


Command Result : No Error


lunacm:>exit
(kskm) root@coen:/media/HSMFD# echo HSM10E
HSM10E
(kskm) root@coen:/media/HSMFD# screencap-verify
█
```

## Place HSM10E (Tier 7) into Secure Transport Mode (STM)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.97 | Using the **LunaCM** terminal, CA executes the following steps:<br>a) Verify the admin partition slot number:<br>`slot list` ✓<br>b) Select the **HSM10E** application partition slot:<br>`slot set -s 3` ✓<br>c) Deactivate the **CO** role:<br>`role deactivate -name co` ✓<br>d) Select the **HSM10E** admin partition slot:<br>`slot set -s 4` ✓<br>e) Log in with the Security Officer role:<br>`role login -name so` ✓<br>f) Follow the instructions on the **HSM10E touchscreen** to perform **SO** authentication:<br>**Note: If the HSM10E touchscreen is off, tap it once to activate the display.**<br>g) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **SO** iKey, then press continue. 5<br>h) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 6<br>i) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue. 3<br>j) When **HSM10E** returns to its dashboard, remove the last iKey of the **SO** set. ✓<br>k) Using the **LunaCM** terminal, place **HSM10E** into STM:<br>`stm transport` ✓<br>l) Type `proceed`, then press enter to continue. ✓<br>m) Verify the **HSM10E** dashboard indicates the device is in **Secure Transport Mode** and the random and verification strings are displayed in the terminal window. ✓ | Y.Y. | 20:33 |

## Print HSM10E Secure Transport Mode (STM) Strings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.98 | CA executes the following steps:<br>a) Exit the **LunaCM** terminal window by typing the following command:<br>`exit` ✓<br>b) Using the **Commands** terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot):<br>`echo HSM10E` ✓<br>c) Print two copies of the STM strings, then verify the screenshot:<br>`screencap-verify` ✓<br>**Note: One copy for the audit bundle and one copy for the HSM10E TEB.**<br>d) Upon successful verification of the screenshot, close the image viewer application. | Y.Y. | 20:34 |

## Place HSM10E (Tier 7) in the TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.99 | CA performs the following steps to prepare **HSM10E** for storage:<br>a) Unplug the HSM cable from the upper USB-C port of **HSM10E**. ✓<br>b) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>c) Read aloud the HSM serial number while the IW verifies it matches the information below. ✓<br>d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. ✓<br>e) Give IW the sealing strips for post-ceremony inventory. ✓<br>f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. ✓<br>g) Initial the TEB along with IW using a ballpoint pen. ✓<br>h) Place the HSM TEB on the cart. ✓<br>**HSM10E: TEB # BB02639623 ✓ / Serial # 712477 ✓** | Y.Y. | 20:35 |

## Ceremony Break

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3.100 | CA divides the participants who desire a ceremony break into groups and ensures the following:<br>a) Remaining participants are sufficient to maintain dual occupancy guidelines for the ceremony room.<br>b) Audit Cameras are never obstructed.<br>c) Live stream audio is muted until the ceremony resumes.<br>RKOS will escort each group of participants out of the ceremony room for the ceremony break. | Y.Y. | 20:36 |
| 3.101 | Once all of the groups have returned to Tier 4 (Ceremony Room) from the break, CA ensures live stream audio is enabled, all participants are present by performing a roll call, then resumes the ceremony. | Y.Y. | 20:51 |

# Root DNSSEC Script Exception

## Exception Details

| Activity | Initials | Time |
|---|---|---|
| IW writes the details of the ceremony exception:<br>Act: 4 Step(s): 2 Page(s): 84<br>Date and time of the exception: 2024/04/26 @ 20:53<br>**Note: IW describes the exception(s) and action(s) below.** | Y.Y. | 20:54. |

The script calls for us to use the wild card describing. the file name and the date. However, we have 2 days worth of log, but we opted to print the log from today only.

**HSMFD SHA-256 HASH** **2024/04/26**

```
 # find -P /media/HSMFD/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wo
rdlist

 SHA-256:    3f1345d57bce8c68062de8eeb628c2381233a505645ec49f9c7a0e1e8c64e192
PGP Words:  cowbell barbecue crusade specialist kickoff sardonic offload gravity afflict cl
ergyman trauma universe Scotland cellulose snapshot consulting atlas concurrent reindeer al
mighty flytrap finicky snowslide opulent python infancy apple Burlington offload getaway te
mpest misnomer
```

```
Script started on 2024-04-26 14:37:19+00:00 [TERM="xterm-256color" TTY="/dev/pts/1" COLUM
NS="72" LINES="23"]
$B3B$?2004h(kskm) root@coen:/media/HSMFD# mkdir HSM9E BHSM1E BHSM2E BHSM1W BHSM2W H
\033[?2004h(kskm) root@coen:/media/HSMFD# lunacm
1088¢M2Ø64±bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->              4
        Label ->
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PW) Key Export With Cloning Mod
e
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, Transport Mode, Zeroized


        Current Slot Id: 4


lunacm:>stm rec\007over -randomuserstring PRHG-HPMS-RSp4-tqdS

        Calculating the verification string (may take up to 3 minutes)...

        Verification String: C53R-PJNE-/RpM-CCp5

        CAUTION:  You are attempting to recover the HSM from Secure Transport Mode.
                  If the verification string does not match the one you were provided out
-of-band,
                  there may be an issue with the HSM. Type 'quit' at the prompt to remain
 in Secure Transport Mode.

                  If the verification strings match, or if you wish to bypass this check,
                  type 'proceed' to recover from Secure Transport Mode.


        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Recovering the HSM from transport...
        Successfully recovered from Transport Mode.

Command Result : No Error


lunacm:>role init -name au


        Not using option -password will initialize au role using PED.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>role login -name au
```

```
Command Result : No Error


lunacm:>audit time sync

HSM time was synchronized to Host

Command Result : No Error


lunacm:>audit config path /media/M\007SMFD/HSM9E

Command Result : No Error


lunacm:>audit configueemak all,failure,success

        You have chosen to log all successful key usage events in symmetric and/or
        asymmetric operations.  This can result in an extremely high volume of log
        messages, which will degrade the overall performance of the HSM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>auditconffgginteeraal hourly@00

Command Result : No Error


lunacm:>audit config size 4096k

Command Result : No Error


lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask         : Log everything
rotation interval  : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log        : /media/HSMFD/HSM9E


Command Result : No Error


lunacm:>hsm init -label HSM9E -iped

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error
```

```
lunacm:>slot list

        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 4

Command Result : No Error


lunacm:>slot set -s 4

        Current Slot Id:    4     (Luna Admin Slot 7.7.2 (PED) Key Export With Cloning Mo
de)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>hsm changgHP -policy 12 -value 0

        You are about to change a destructive HSM policy.
        All partitions of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed
hsm changeHP
Command Result : No Error


lunacm:>hsm changeHP -policy 21 -value 0

Command Result : No Error


lunacm:>hsm showinfo

        Slot Id -> 4
        Partition Label -> HSM9E
        Partition Serial Number -> 712482
        Partition Model -> Luna G7
        Partition Manufacturer ->
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in
        RPV Initialized -> No
```

```
        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: 1e0000000500000222df0a00


        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             24408

        System Times:
                HSM  : Fri Apr 26 15:07:14 UTC 2024
                Host : Fri Apr 26 15:07:15 UTC 2024
                Difference: 1 sec

        HSM Storage:
                Total Storage Space:  33554432
                Used Storage Space:   679768
                Free Storage Space:   32874664
                Allowed Partitions:   1
                Number of Partitions: 0

        HSM Part Number -> 808-000080-001

        Environmental:
                System Temperature :  42 deg. C

        Firmware Version -> 7.7.2
        Bootloader Version ->  1.6.0
        Rollback Firmware Version -> Not Available

        License Count:
                1. 621000186-000 G7 Base CUF with Real Certificate

        *** The HSM is in FIPS approved operation mode. ***

Command Result : No Error


lunacm:>partition create

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 4

Command Result : No Error

lunacm:>slot set -s 3

        Current Slot Id:    3      (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error

lunacm:>partition init -label HSM9E_KSK-2024

        You are about to initialize the partition.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error

lunacm:>role login -name po

        Please attend to the PED.

Command Result : No Error

lunacm:>partition changepoligy -policy 22 -value 1

Command Result : No Error

lunacm:>role init -name co

        Please attend to the PED.

Command Result : No Error

lunacm:>role createchallenge -name co

        Please attend to the PED.

        enter new challenge secret: ********

        re-enter new challenge secret: ********

Command Result : No Error

lunacm:>role logout

Command Result : No Error

lunacm:>role login -name co

        enter password: ********

        Please attend to the PED.

Command Result : No Error

lunacm:>exit
\033[?2004h(kskm) root@coen:/media/HSMFD# cd /media/HSMFD/KS\007K53-2
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# ksk\007m\007-k\007eymaster -hhsm-luna k
eygego\007rithm RSASHA256 --size 2048
2024-04-26117:30:35,393: kskm.common.config: INFO Loaded configuration from file ksrsigne
r.yaml SHA-256 5a2ff2646e14ab6883fd972faf9baf1cd91c237a01df738b1f9288a6449ed3ec WORDS enl
ist combustion uproot getaway goldfish belowground rhythm gravity Mohawk Wyoming preshrun
k combustion rocker Norwegian rocker Brazilian sugar Brazilian blowtorch infancy absurd t
herapist hockey Medusa billiard misnomer newborn paragon crumpled onlooker stapler unicor
n
2024-04-26 17:30:35,430: kskm.common.config: INFO Configuration validated
2024-04-26 17:30:35,430: kskm.misc.hsm: INFO Initializing PKCS#11 module luna using /usr/
safenet/lunaclient/lib/libCryptoki2_64.so
2024-04-26 17:30:35,662: kskm.misc.hsm: INFO HSM First slot:      HSM9E_KSK-2024

2024-04-26 17:30:35,663: kskm.misc.hsm: INFO HSM ManufacturerID:

2024-04-26 17:30:35,663: kskm.misc.hsm: INFO HSM Model:           Luna G7
2024-04-26 17:30:35,663: kskm.misc.hsm: INFO HSM Serial:          1658876115494
2024-04-26 17:30:35,663: kskm.tools.keymaster: INFO Generate key
2024-04-26 17:30:36,076: kskm.keymaster.keygen: INFO Generated key: key_label=Kmyv6jo alg
=RSA bits=2048 exp=65537
2024-04-26 17:30:36,077: kskm.tools.keymaster: INFO Generated key Kmyv6jo has key tag 386
96 for algorithm=AlgorithmDNSSEC.RSASHA256, flags=0x101
2024-04-26 17:30:36,077: kskm.tools.keymaster: INFO Generated key Kmyv6jo has key tag 388
24 with the REVOKE bit set (flags 0x181)
2024-04-26 17:30:36,078: kskm.tools.keymaster: INFO DS record for generated key:
. IN DS 38696 8 2 683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16
>> frighten crucifix button Apollo spheroid megaton puppy hideaway brickyard bottomless d
eadbolt pioneer lockup hydraulic atlas bottomless breakup microscope allow detector ancie
nt frequency Burbank dictator cleanup Virginia crumpled Pandora slowdown Wichita briefcas
e bodyguard
k033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# kskm-k\007eymaster --hsm luna invento
2024-04-26117:30:48,550: kskm.common.config: INFO Loaded configuration from file ksrsigne
r.yaml SHA-256 5a2ff2646e14ab6883fd972faf9baf1cd91c237a01df738b1f9288a6449ed3ec WORDS enl
ist combustion uproot getaway goldfish belowground rhythm gravity Mohawk Wyoming preshrun
k combustion rocker Norwegian rocker Brazilian sugar Brazilian blowtorch infancy absurd t
herapist hockey Medusa billiard misnomer newborn paragon crumpled onlooker stapler unicor
n
2024-04-26 17:30:48,587: kskm.common.config: INFO Configuration validated
```

```
2024-04-26 17:30:48,587: kskm.misc.hsm: INFO Initializing PKCS#11 module luna using /usr/
safenet/lunaclient/lib/libCryptoki2_64.so
2024-04-26 17:30:48,816: kskm.misc.hsm: INFO HSM First slot:      HSM9E_KSK-2024

2024-04-26 17:30:48,816: kskm.misc.hsm: INFO HSM ManufacturerID:

2024-04-26 17:30:48,816: kskm.misc.hsm: INFO HSM Model:           Luna G7
2024-04-26 17:30:48,816: kskm.misc.hsm: INFO HSM Serial:          1658876115494
2024-04-26 17:30:48,817: kskm.tools.keymaster: INFO Show HSM inventory
2024-04-26 17:30:48,824: kskm.tools.keymaster: INFO Key inventory:
HSM luna:
  Slot 3:
    Signing key pairs:
      Kmyv6jo alg=RSA bits=2048 exp=65537 -- Matching KSK not found in configuration
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# prin\007tlog kskm-k\007eymaster-2024042
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-20240426240426\033[K
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-20240426l
\033[B\033[Bcopies value 0.
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-202404*.lo
\033[B\033[Bcopies value 0.
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-2024042024*.lo033[K
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-20240426240426\033[K
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-2024042024261033[K
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog\007kskm-keymaster-202404*.
kskm-keymaster-20240426-173035-995.log  ksrsigner.yaml
kskm-keymaster-20240426-173048-997.log
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-\007keymaster-20240426\033[K
\033[K\033[A(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-keymaster-20240426-
\033[B\033[B0411 copy ] sent to printer
2 lines were wrapped
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# printlog kskm-\007keymaster-20240426-1
\033[B\033[B0411 copy ] sent to printer
1 line was wrapped
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# lunacm
lunacm (64-bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


      Available HSMs:

      Slot Id ->                 3
      Label ->                   HSM9E_KSK-2024
      Serial Number ->           1658876115494
      Model ->                   Luna G7
      Firmware Version ->        7.7.2
      Bootloader Version ->      1.6.0
      Configuration ->           Luna User Partition With SO (PED) Key Export With Cloning
Mode
      Slot Description ->        User Token Slot


      Slot Id ->                 4
      Label ->                   HSM9E
      Serial Number ->           712482
      Model ->                   Luna G7
      Firmware Version ->        7.7.2
      Bootloader Version ->      1.6.0
      Configuration ->           Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
      Slot Description ->        Admin Token Slot
      HSM Status ->              L3 Device, OK
```

```
      Slot Id ->                 105
      Label ->
      Serial Number ->           706530
      Model ->                   Luna G7
      Firmware Version ->        7.7.2
      Bootloader Version ->      1.6.0
      Configuration ->           Luna HSM Admin Partition (PW) Backup Mode
      Slot Description ->        Admin Token Slot
      HSM Status ->              L3 Device, Transport Mode, Zeroized


      Current Slot Id: 3


lunacm:>slot set -s 105

      Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PW) Backup Device)

Command Result : No Error


lunacm:>stm recover -randomuserstring SR9K-qqTM-5K55-KdNx

      Calculating the verification string (may take up to 3 minutes)...

      Verification String: JWA6-CSLT-WWXY-pETb

      CAUTION:  You are attempting to recover the HSM from Secure Transport Mode.
                If the verification string does not match the one you were provided out
-of-band,
                there may be an issue with the HSM. Type 'quit' at the prompt to remain
 in Secure Transport Mode.

                If the verification strings match, or if you wish to bypass this check,
                type 'proceed' to recover from Secure Transport Mode.


      Are you sure you wish to continue?

      Type 'proceed' to continue, or 'quit' to quit now ->proceed

      Recovering the HSM from transport...
      Successfully recovered from Transport Mode.

Command Result : No Error


lunacm:>role init -name au


      Not using option -password will initialize au role using PED.
      Are you sure you wish to continue?

      Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>role login -name au

Command Result : No Error
```

```
lunacm:>audit time sync

HSM time was synchronized to Host

Command Result : No Error


lunacm:>audit oonfig path /media/HSMFD/BHSM1E

Command Result : No Error


lunacm:>audit config evmask all,failure,success

        You have chosen to log all successful key usage events in symmetric and/or
        asymmetric operations.  This can result in an extremely high volume of log
        messages, which will degrade the overall performance of the HSM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>audit config interval hourly@00

Command Result : No Error


lunacm:>audit aonfig size 4096k

Command Result : No Error


lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask         : Log everything
rotation interval : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log        : /media/HSMFD/BHSM1E


Command Result : No Error


lunacm:>hsm init -label BHSM1E -iped

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error


lunacm:>slot list
```

```
        Slot Id ->                  3
        Label ->                    HSM9E_KSK-2024
        Serial Number ->            1658876115494
        Model ->                    Luna G7
        Firmware Version ->         7.7.2
        Bootloader Version ->       1.6.0
        Configuration ->            Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->         User Token Slot


        Slot Id ->                  4
        Label ->                    HSM9E
        Serial Number ->            712482
        Model ->                    Luna G7
        Firmware Version ->         7.7.2
        Bootloader Version ->       1.6.0
        Configuration ->            Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->         Admin Token Slot
        HSM Status ->               L3 Device, OK


        Slot Id ->                  105
        Label ->                    BHSM1E
        Serial Number ->            706530
        Model ->                    Luna G7
        Firmware Version ->         7.7.2
        Bootloader Version ->       1.6.0
        Configuration ->            Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->         Admin Token Slot
        HSM Status ->               L3 Device, OK


        Current Slot Id: 105


Command Result : No Error


lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PED) Backup Device)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>hsm changehsmpolicy -poligy 55--value 1

Command Result : No Error


lunacm:>hsm showinfo

        Slot Id -> 105
        Partition Label -> BHSM1E
        Partition Serial Number -> 706530
        Partition Model -> Luna G7
        Partition Manufacturer ->
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in
        RPV Initialized -> No

        Partition Cloning Version -> 1
        Partition FM Status -> FM Disabled

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: Not Initialized


        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             24408

        System Times:
                HSM  : Fri Apr 26 18:00:41 UTC 2024
                Host : Fri Apr 26 18:00:41 UTC 2024
                Difference: 0 sec

        HSM Storage:
                Total Storage Space:  33816576
                Used Storage Space:   679768
                Free Storage Space:   33136808
                Allowed Partitions:   100
                Number of Partitions: 0

        HSM Part Number -> 808-000080-001

        Environmental:
                System Temperature :  36 deg. C

        Firmware Version -> 7.7.2
        Bootloader Version ->  1.6.0
        Rollback Firmware Version -> Not Available

        License Count:
                1. 621000247-000 G7 BU 32M Base Configuration (32MB/100Partitions)

        *** The HSM is in FIPS approved operation mode. ***

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
```

```
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM1E
        Serial Number ->        706530
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK



        Current Slot Id: 105


Command Result : No Error


lunacm:>slot set -s 3

        Current Slot Id:    3     (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error


lunacm:>role login -name so
Error: parsing for parameter '-name' reports 'invalid parameter'.

  This command will log a role into a partition.
  The following options are available:

  Options             Short    Description

  ------------------------------------------

  -name               -n       name of role logging in

  -password           -p       password for role


  Syntax: role login -name <string> [-password <string>]

Command Result : 0x4 (Invalid arguments)


lunacm:>role login -name so
```

```
        enter password: ********

 Command Result : No Error

 lunacm:>partition contents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          Kmyv6jo
        Handle:         83
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00

        Number of objects:  2

 Command Result : No Error

 lunacm:>pa8t1028paatchice backape-backup05s±part06iepaK8Kt2024

        Logging in as the SO on slot 105.

        Please attend to the PED.

        Creating partition KSK-2024 on slot 105.

        Please attend to the PED.

        Verifying that all objects can be backed up...

        2 objects will be backed up.

        Backing up objects...
        Cloned object 83 to partition KSK-2024 (new handle 75).
        Cloned object 80 to partition KSK-2024 (new handle 80).

        Resizing partition KSK-2024 on slot 105 to minimum necessary space.

        Backup Successfully Completed.

        2 objects have been backed up to partition KSK-2024
        on slot 105.
 Command Result : No Error

 lunacm:>partition archive list -slot1185
```

```
        HSM Storage Information for slot 105:

           Total HSM Storage Space: 33816576
           Used HSM Storage Space:  705868
           Free HSM Storage Space:  33110708
           Allowed Partitions:      100
           Number Of Partitions:    1

        Partition list for slot 105

           Number of partitions: 1

           Slot Id:                   5
           Label:                     KSK-2024
           Total Storage Size:        1884
           Used Storage Size:         1884
           Free Storage Size:         0
           Number Of Objects:         2

           Partition Cloning Version: 3
           Partition FM Status:       FM Disabled

           Partition SMK OUIDs:
                   SMK-FW4: Not Initialized
                   SMK-FW6: Not Initialized
                   SMK-FW7-FM: Not Initialized
                   SMK-FW7-Rollover: Not Initialized
                   SMK-FW7-Primary: Not Initialized


 Command Result : No Error


 lunacm:>partition archive contents -slot 105 -partition KSK-2024

        Logging in as the user on slot 105.

        Please attend to the PED.

        Contents of partition KSK-2024 on slot 105 :

        Object list:

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         75
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00

        Number of objects:  2

 Command Result : No Error

 lunacm:>exit
```

```
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# lunacm
1088¢M2@84±bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.

        Available HSMs:

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->
        Serial Number ->        718029
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PW) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, Transport Mode, Zeroized


        Current Slot Id: 3

lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PW) Backup Device)

Command Result : No Error

lunacm:>stm recover -randomuserstring MJ3F-KAF3-CxtL-STJE

        Calculating the verification string (may take up to 3 minutes)...

        Verification String: KpJ4-6YEA-SXRq-4Ebq

        CAUTION:  You are attempting to recover the HSM from Secure Transport Mode.
                  If the verification string does not match the one you were provided out
-of-band,
                  there may be an issue with the HSM. Type 'quit' at the prompt to remain
 in Secure Transport Mode.

                  If the verification strings match, or if you wish to bypass this check,
                  type 'proceed' to recover from Secure Transport Mode.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Recovering the HSM from transport...
        Successfully recovered from Transport Mode.

Command Result : No Error

lunacm:>role init--name au

        Not using option -password will initialize au role using PED.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error

lunacm:>role login -name au

Command Result : No Error

lunacm:>audit time sgnc

HSM time was synchronized to Host

Command Result : No Error

lunacm:>audit config path /media/HSMBB/BHSM2E

Command Result : No Error

lunacm:>audit config evmask all,fálhnee,success

        You have chosen to log all successful key usage events in symmetric and/or
        asymmetric operations.  This can result in an extremely high volume of log
        messages, which will degrade the overall performance of the HSM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error

lunacm:>audit config interval hourly@00

Command Result : No Error

lunacm:>audit config size 8096k

Command Result : No Error

lunacm:>audit config get
```

```
Current Logging Configuration
-----------------------------
event mask          : Log everything
rotation interval : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log          : /media/HSMFD/BHSM2E

Command Result : No Error


lunacm:>hsm init -label BHSM2E -iped

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2E
        Serial Number ->        718029
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 105
```

```
Command Result : No Error


lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PED) Backup Device)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>hsm changehsmpolicy -policy 55 -value 1

Command Result : No Error


lunacm:>hsm showinfo

        Slot Id -> 105
        Partition Label -> BHSM2E
        Partition Serial Number -> 718029
        Partition Model -> Luna G7
        Partition Manufacturer ->
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in
        RPV Initialized -> No

        Partition Cloning Version -> 1
        Partition FM Status -> FM Disabled

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: Not Initialized


        Partition Storage:
                Total Storage Space:   655360
                Used Storage Space:    0
                Free Storage Space:    655360
                Object Count:          0
                Overhead:              24408

        System Times:
                HSM  : Fri Apr 26 18:36:11 UTC 2024
                Host : Fri Apr 26 18:36:11 UTC 2024
                Difference: 0 sec

        HSM Storage:
                Total Storage Space:   33816576
                Used Storage Space:    679768
                Free Storage Space:    33136808
                Allowed Partitions:    100
                Number of Partitions: 0

        HSM Part Number -> 808-000080-001

        Environmental:
                System Temperature :  38 deg. C

        Firmware Version -> 7.7.2
        Bootloader Version ->  1.6.0
        Rollback Firmware Version -> Not Available

        License Count:
                1. 621000247-000 G7 BU 32M Base Configuration (32MB/100Partitions)

        *** The HSM is in FIPS approved operation mode. ***

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2E
        Serial Number ->        718029
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 105

Command Result : No Error

lunacm:>slot set -s 3
```

```
        Current Slot Id:    3     (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error

lunacm:>role login -name co


        enter password: ********


Command Result : No Error


lunacm:>partitioncontents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          Kmyv6jo
        Handle:         83
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a000000500000222df0a00


        Number of objects:  2

Command Result : No Error


lunacm:>partibion archive backup -slot 105 -partition KSK-2024

        Logging in as the SO on slot 105.

        Please attend to the PED.

        Creating partition KSK-2024 on slot 105.

        Please attend to the PED.

        Verifying that all objects can be backed up...

        2 objects will be backed up.

        Backing up objects...
        Cloned object 83 to partition KSK-2024 (new handle 75).
        Cloned object 80 to partition KSK-2024 (new handle 80).

        Resizing partition KSK-2024 on slot 105 to minimum necessary space.

        Backup Successfully Completed.

        2 objects have been backed up to partition KSK-2024
        on slot 105.

 Command Result : No Error


 lunacm:>partition archive list -slot 105

         HSM Storage Information for slot 105:

            Total HSM Storage Space: 33816576
            Used HSM Storage Space:  705868
            Free HSM Storage Space:  33110708
            Allowed Partitions:      100
            Number Of Partitions:    1

         Partition list for slot 105

            Number of partitions: 1

            Slot Id:                  5
            Label:                   KSK-2024
            Total Storage Size:       1884
            Used Storage Size:        1884
            Free Storage Size:        0
            Number Of Objects:        2

            Partition Cloning Version: 3
            Partition FM Status:      FM Disabled

            Partition SMK OUIDs:
                    SMK-FW4: Not Initialized
                    SMK-FW6: Not Initialized
                    SMK-FW7-FM: Not Initialized
                    SMK-FW7-Rollover: Not Initialized
                    SMK-FW7-Primary: Not Initialized


 Command Result : No Error


 lunacm:>partitionaarchive contents -slot1105 -partition KSK-2024

         Logging in as the user on slot 105.

         Please attend to the PED.

         Contents of partition KSK-2024 on slot 105 :

         Object list:

         Label:         Kmyv6jo
         Handle:        80
         Object Type:   Public Key
         Usage Limit:   none
         Object UID:    3a000000500000222df0a00

         Label:         Kmyv6jo
         Handle:        75
         Object Type:   Private Key
         Usage Limit:   none
         Object UID:    3b000000500000222df0a00
```

```
         Number of objects:  2


 Command Result : No Error


 lunacm:>exit
 \033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# lunacm
 1033¢M2004‡bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


         Available HSMs:

         Slot Id ->              3
         Label ->                HSM9E_KSK-2024
         Serial Number ->        1658876115494
         Model ->                Luna G7
         Firmware Version ->     7.7.2
         Bootloader Version ->   1.6.0
         Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
  Mode
         Slot Description ->     User Token Slot


         Slot Id ->              4
         Label ->                HSM9E
         Serial Number ->        712482
         Model ->                Luna G7
         Firmware Version ->     7.7.2
         Bootloader Version ->   1.6.0
         Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
 de
         Slot Description ->     Admin Token Slot
         HSM Status ->           L3 Device, OK


         Slot Id ->              105
         Label ->
         Serial Number ->        718041
         Model ->                Luna G7
         Firmware Version ->     7.7.2
         Bootloader Version ->   1.6.0
         Configuration ->        Luna HSM Admin Partition (PW) Backup Mode
         Slot Description ->     Admin Token Slot
         HSM Status ->           L3 Device, Transport Mode, Zeroized



         Current Slot Id: 3


 lunacm:>slot set -s 105

         Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PW) Backup Device)

 Command Result : No Error


 lunacm:>stm recover -randomuserstring GR9G-qppHAAMqT-9WTA

         Calculating the verification string (may take up to 3 minutes)...

         Verification String: EKtF-GN6W-5YJx-RHWN
```

```
        CAUTION:  You are attempting to recover the HSM from Secure Transport Mode.
                  If the verification string does not match the one you were provided out
-of-band,
                  there may be an issue with the HSM. Type 'quit' at the prompt to remain
 in Secure Transport Mode.

                  If the verification strings match, or if you wish to bypass this check,
                  type 'proceed' to recover from Secure Transport Mode.


        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Recovering the HSM from transport...
        Successfully recovered from Transport Mode.

Command Result : No Error


lunacm:>role init -name au


        Not using option -password will initialize au role using PED.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>role login -name au

Command Result : No Error


lunacm:>audit aime sync

HSM time was synchronized to Host

Command Result : No Error


lunacm:>audit config path /media/HSMFD/BHSM1W

Command Result : No Error


lunacm:>audit config evmask all,failure,success

        You have chosen to log all successful key usage events in symmetric and/or
        asymmetric operations.  This can result in an extremely high volume of log
        messages, which will degrade the overall performance of the HSM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->þ807proceed

Command Result : No Error


lunacm:>audit config interval hourly@00

Command Result : No Error
```

```
lunacm:>audit config size 4096k

Command Result : No Error


lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask          : Log everything
rotation interval : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log         : /media/HSMFD/BHSM1W


Command Result : No Error


lunacm:>hsm init -labeè BHSM1W -iped

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM1W
        Serial Number ->        718041
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->          Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->       Admin Token Slot
        HSM Status ->             L3 Device, OK


        Current Slot Id: 105

Command Result : No Error


lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PED) Backup Device)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>hsm changehsmpolicy -pòlicy 55 -value 1

Command Result : No Error


lunacm:>hsm showinfo

        Slot Id -> 105
        Partition Label -> BHSM1W
        Partition Serial Number -> 718041
        Partition Model -> Luna G7
        Partition Manufacturer ->
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in
        RPV Initialized -> No

        Partition Cloning Version -> 1
        Partition FM Status -> FM Disabled

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: Not Initialized


        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             24408

        System Times:
                HSM  : Fri Apr 26 19:01:49 UTC 2024
                Host : Fri Apr 26 19:01:49 UTC 2024
```

```
                Difference: 0 sec

        HSM Storage:
                Total Storage Space:  33816576
                Used Storage Space:   679768
                Free Storage Space:   33136808
                Allowed Partitions:   100
                Number of Partitions: 0

        HSM Part Number -> 808-000080-001

        Environmental:
                System Temperature :  37 deg. C

        Firmware Version -> 7.7.2
        Bootloader Version ->  1.6.0
        Rollback Firmware Version -> Not Available

        License Count:
                1. 621000247-000 G7 BU 32M Base Configuration (32MB/100Partitions)

        *** The HSM is in FIPS approved operation mode. ***

Command Result : No Error


lunacm:>sàot list

        Slot Id ->                3
        Label ->                  HSM9E_KSK-2024
        Serial Number ->          1658876115494
        Model ->                  Luna G7
        Firmware Version ->       7.7.2
        Bootloader Version ->     1.6.0
        Configuration ->          Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->       User Token Slot


        Slot Id ->                4
        Label ->                  HSM9E
        Serial Number ->          712482
        Model ->                  Luna G7
        Firmware Version ->       7.7.2
        Bootloader Version ->     1.6.0
        Configuration ->          Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->       Admin Token Slot
        HSM Status ->             L3 Device, OK


        Slot Id ->                105
        Label ->                  BHSM1W
        Serial Number ->          718041
        Model ->                  Luna G7
        Firmware Version ->       7.7.2
        Bootloader Version ->     1.6.0
        Configuration ->          Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->       Admin Token Slot
        HSM Status ->             L3 Device, OK


        Current Slot Id: 105
```

```
Command Result : No Error


lunacm:>slot set -s 103

        The specified slot number is invalid.

Command Result : 0x3 (CKR_SLOT_ID_INVALID)


lunacm:>slot set -s 303

        Current Slot Id:    3      (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error


lunacm:>role login -name co

        enter password: ********

Command Result : No Error


lunacm:>phowition contents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          Kmyv6jo
        Handle:         83
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00


        Number of objects:  2

Command Result : No Error


lunacm:>partition archive backup -slot 105 -partition KSK-2024

        Logging in as the SO on slot 105.

        Please attend to the PED.

        Creating partition KSK-2024 on slot 105.

        Please attend to the PED.
```

```
        Verifying that all objects can be backed up...

        2 objects will be backed up.

        Backing up objects...
        Cloned object 83 to partition KSK-2024 (new handle 75).
        Cloned object 80 to partition KSK-2024 (new handle 80).

        Resizing partition KSK-2024 on slot 105 to minimum necessary space.

        Backup Successfully Completed.

        2 objects have been backed up to partition KSK-2024
        on slot 105.

Command Result : No Error


lunacm:>partition archive list -slot 105

        HSM Storage Information for slot 105:

           Total HSM Storage Space:  33816576
           Used HSM Storage Space:   705868
           Free HSM Storage Space:   33110708
           Allowed Partitions:       100
           Number Of Partitions:     1

        Partition list for slot 105

           Number of partitions: 1

           Slot Id:                   5
           Label:                     KSK-2024
           Total Storage Size:        1884
           Used Storage Size:         1884
           Free Storage Size:         0
           Number Of Objects:         2

           Partition Cloning Version: 3
           Partition FM Status:       FM Disabled

           Partition SMK OUIDs:
                   SMK-FW4: Not Initialized
                   SMK-FW6: Not Initialized
                   SMK-FW7-FM: Not Initialized
                   SMK-FW7-Rollover: Not Initialized
                   SMK-FW7-Primary: Not Initialized



Command Result : No Error


lunacm:>partition archive contents -slot 105 -partition KSK-2024

        Logging in as the user on slot 105.

        Please attend to the PED.

        Contents of partition KSK-2024 on slot 105 :

        Object list:
```

```
        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         75
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00


        Number of objects:  2


Command Result : No Error


lunacm:>slot list

        Slot Id ->                    3
        Label ->                      HSM9E_KSK-2024
        Serial Number ->              1658876115494
        Model ->                      Luna G7
        Firmware Version ->           7.7.2
        Bootloader Version ->         1.6.0
        Configuration ->              Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->           User Token Slot


        Slot Id ->                    4
        Label ->                      HSM9E
        Serial Number ->              712482
        Model ->                      Luna G7
        Firmware Version ->           7.7.2
        Bootloader Version ->         1.6.0
        Configuration ->              Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->           Admin Token Slot
        HSM Status ->                 L3 Device, OK


        Slot Id ->                    105
        Label ->                      BHSM1W
        Serial Number ->              718041
        Model ->                      Luna G7
        Firmware Version ->           7.7.2
        Bootloader Version ->         1.6.0
        Configuration ->              Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->           Admin Token Slot
        HSM Status ->                 L3 Device, OK


        Current Slot Id: 3

Command Result : No Error


lunacm:>slot set -s 105
```

```
        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PED) Backup Device)

Command Result : No Error


lunacm:>fole login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: PFPP-YAtq-CWAT-Ht/Y


         Random User String: bt/J-HpGW-MJsp-E5Yt


Command Result : No Error


lunacm:>exit
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# \007echo BHSM1W
NBSM[W20041
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# screencap-verify
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# lunacm
\033¢M2@64±bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->                    3
        Label ->                      HSM9E_KSK-2024
        Serial Number ->              1658876115494
        Model ->                      Luna G7
        Firmware Version ->           7.7.2
        Bootloader Version ->         1.6.0
        Configuration ->              Luna User Partition With SO (PED) Key Export With Cloning
Mode
        Slot Description ->           User Token Slot


        Slot Id ->                    4
        Label ->                      HSM9E
        Serial Number ->              712482
        Model ->                      Luna G7
        Firmware Version ->           7.7.2
        Bootloader Version ->         1.6.0
        Configuration ->          Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->       Admin Token Slot
        HSM Status ->             L3 Device, OK


        Slot Id ->                105
        Label ->
        Serial Number ->          718018
        Model ->                  Luna G7
        Firmware Version ->       7.7.2
        Bootloader Version ->     1.6.0
        Configuration ->          Luna HSM Admin Partition (PW) Backup Mode
        Slot Description ->       Admin Token Slot
        HSM Status ->             L3 Device, Transport Mode, Zeroized


        Current Slot Id: 3


lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PW) Backup Device)

Command Result : No Error


lunacm:>stm recover -randomaberstring 3bxs-JNdd-Ctd4-H5/s

        Calculating the verification string (may take up to 3 minutes)...

        Verification String: KqY5-C7WA-LbxJ-TqCW

        CAUTION:  You are attempting to recover the HSM from Secure Transport Mode.
                  If the verification string does not match the one you were provided out
-of-band,
                  there may be an issue with the HSM. Type 'quit' at the prompt to remain
 in Secure Transport Mode.

                  If the verification strings match, or if you wish to bypass this check,
                  type 'proceed' to recover from Secure Transport Mode.


        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Recovering the HSM from transport...
        Successfully recovered from Transport Mode.

Command Result : No Error


lunacm:>role init -name au


        Not using option -password will initialize au role using PED.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error
```

```
lunacm:>role login -name au

Command Result : No Error


lunacm:>audit timessync

HSM time was synchronized to Host

Command Result : No Error


lunacm:>audit config path /media/HSMFD/BHSM2W

Command Result : No Error


lunacm:>audit config evmask all,fáàlùre,succees

        You have chosen to log all successful key usage events in symmetric and/or
        asymmetric operations.  This can result in an extremely high volume of log
        messages, which will degrade the overall performance of the HSM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>audit config interval hourly@00

Command Result : No Error


lunacm:>audit config size 4096k

Command Result : No Error


lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask         : Log everything
rotation interval : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log        : /media/HSMFD/BHSM2W


Command Result : No Error


lunacm:>hsm init--labèlBHHSM2W -iped

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.
```

```
Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK



        Current Slot Id: 105

Command Result : No Error


lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PED) Backup Device)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>hsm changehsmpolicy -policy 55 -value 1

Command Result : No Error
```

```
lunacm:>hsm showinfo

        Slot Id -> 105
        Partition Label -> BHSM2W
        Partition Serial Number -> 718018
        Partition Model -> Luna G7
        Partition Manufacturer ->
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in
        RPV Initialized -> No

        Partition Cloning Version -> 1
        Partition FM Status -> FM Disabled

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: Not Initialized


        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             24408

        System Times:
                HSM  : Fri Apr 26 19:37:27 UTC 2024
                Host : Fri Apr 26 19:37:27 UTC 2024
                Difference: 0 sec

        HSM Storage:
                Total Storage Space:  33816576
                Used Storage Space:   679768
                Free Storage Space:   33136808
                Allowed Partitions:   100
                Number of Partitions: 0

        HSM Part Number -> 808-000080-001

        Environmental:
                System Temperature :  38 deg. C

        Firmware Version -> 7.7.2
        Bootloader Version ->  1.6.0
        Rollback Firmware Version -> Not Available

        License Count:
                1. 621000247-000 G7 BU 32M Base Configuration (32MB/100Partitions)

        *** The HSM is in FIPS approved operation mode. ***

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->         1658876115494
        Model ->                 Luna G7
        Firmware Version ->      7.7.2
        Bootloader Version ->    1.6.0
        Configuration ->         Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->      User Token Slot


        Slot Id ->               4
        Label ->                 HSM9E
        Serial Number ->         712482
        Model ->                 Luna G7
        Firmware Version ->      7.7.2
        Bootloader Version ->    1.6.0
        Configuration ->         Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->      Admin Token Slot
        HSM Status ->            L3 Device, OK


        Slot Id ->               105
        Label ->                 BHSM2W
        Serial Number ->         718018
        Model ->                 Luna G7
        Firmware Version ->      7.7.2
        Bootloader Version ->    1.6.0
        Configuration ->         Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->      Admin Token Slot
        HSM Status ->            L3 Device, OK


        Current Slot Id: 105

Command Result : No Error

lunacm:>slot set -s 3

        Current Slot Id:    3    (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error

lunacm:>role login -name co

        enter password: ********

Command Result : No Error

lunacm:>partition contents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          Kmyv6jo
        Handle:         83
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00


        Number of objects:  2

Command Result : No Error

lunacm:>p887pachiaion archive backup -slot 105 -partition KSK-2024

        Logging in as the SO on slot 105.

        Please attend to the PED.

        Creating partition KSK-2024 on slot 105.

        Please attend to the PED.

        Verifying that all objects can be backed up...

        2 objects will be backed up.

        Backing up objects...
        Cloned object 83 to partition KSK-2024 (new handle 75).
        Cloned object 80 to partition KSK-2024 (new handle 80).

        Resizing partition KSK-2024 on slot 105 to minimum necessary space.

        Backup Successfully Completed.

        2 objects have been backed up to partition KSK-2024
        on slot 105.

Command Result : No Error

lunacm:>partition archive list -slot 105

        HSM Storage Information for slot 105:

           Total HSM Storage Space: 33816576
           Used HSM Storage Space:  705868
           Free HSM Storage Space:  33110708
           Allowed Partitions:      100
           Number Of Partitions:    1

        Partition list for slot 105

           Number of partitions: 1

           Slot Id:                  5
           Label:                    KSK-2024
           Total Storage Size:       1884
           Used Storage Size:        1884
```

```
          Free Storage Size:          0
          Number Of Objects:          2

          Partition Cloning Version: 3
          Partition FM Status:        FM Disabled

          Partition SMK OUIDs:
                  SMK-FW4: Not Initialized
                  SMK-FW6: Not Initialized
                  SMK-FW7-FM: Not Initialized
                  SMK-FW7-Rollover: Not Initialized
                  SMK-FW7-Primary: Not Initialized


Command Result : No Error


lunacm:>partition archive content -slot 105 -partition KSK-2024

  These commands can be used to query other backup devices or
  backup/restore objects to/from backup devices.


  Command         Short   Description
  ------------------------------------

  backup          b       Backup objects from the current slot to a backup
                          device. Also used to backup SKS Master Key (SMK).
  restore         r       Restore objects from the backup device to the current
                          slot. Also used to restore SKS Master Key (SMK).
  list            l       List the backup partitions on a backup device.
  contents        c       List the contents of a backup partition in a backup
                          device.
  delete          d       Delete the specified backup partition in a backup
                          device.

  Syntax:
        partition archive backup
        partition archive restore
        partition archive list
        partition archive contents
        partition archive delete


Command Result : 0x1 (Unknown command)


lunacm:>partition archive contents-s$ott1085-ppartttionnKSKK22224

        Logging in as the user on slot 105.

        Please attend to the PED.

        Contents of partition KSK-2024 on slot 105 :

        Object list:

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00
```

```
        Label:          Kmyv6jo
        Handle:         75
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00


        Number of objects:  2


Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM9E_KSK-2024
        Serial Number ->        1658876115494
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM9E
        Serial Number ->        712482
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 3


Command Result : No Error


lunacm:>slot set -s 3

        Current Slot Id:    3    (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error
```

```
lunacm:>role deactivate -name co

Command Result : No Error


lunacm:>slot set -s 4

        Current Slot Id:    4      (Luna Admin Slot 7.7.2 (PED) Key Export With Cloning Mo
de)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: /CKG-NJ77-EF75-SHpJ


         Random User String: YTXs-JLML-HdRM-LGMG


Command Result : No Error


lunacm:>exit
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# echo HSM9E
NS89E?20041
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# screencap-verify
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# lunac
b83R{?20B4c: command not found
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# lunacm
\C8a¢m2@64=bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->              4
        Label ->
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PW) Key Export With Cloning Mod
e
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, Transport Mode, Zeroized


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 4


lunacm:>slot set -s 4

        Current Slot Id:    4      (Luna Admin Slot 7.7.2 (PW) Key Export With Cloning Mod
e)

Command Result : No Error


lunacm:>stm recover -randomuserstring 4xp5-WtJx-THSP-A46W

        Calculating the verification string (may take up to 3 minutes)...

        Verification String: 3t/x-CWpX-p5NW-TEKA

        CAUTION:  You are attempting to recover the HSM from Secure Transport Mode.
                  If the verification string does not match the one you were provided out
-of-band,
                  there may be an issue with the HSM. Type 'quit' at the prompt to remain
 in Secure Transport Mode.

                  If the verification strings match, or if you wish to bypass this check,
                  type 'proceed' to recover from Secure Transport Mode.


        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Recovering the HSM from transport...
        Successfully recovered from Transport Mode.

Command Result : No Error


lunacm:>role init -name au


        Not using option -password will initialize au role using PED.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error
```

```
lunacm:>ròèe login -name au

Command Result : No Error


lunacm:>audit time sync

HSM time was synchronized to Host

Command Result : No Error


lunacm:>audEtconffig path /media/MSMFD/HSM10E

Command Result : No Error


lunacm:>audit config evmask all,failure,success

        You have chosen to log all successful key usage events in symmetric and/or
        asymmetric operations.  This can result in an extremely high volume of log
        messages, which will degrade the overall performance of the HSM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>audit config interval hourly@00

Command Result : No Error


lunacm:>audit config size 4096k

Command Result : No Error


lunacm:>audit config get

Current Logging Configuration
-----------------------------
event mask        : Log everything
rotation interval : hourly@ 0 minutes past the hour
rotation size (MB): 4
path to log       : /media/HSMFD/HSM10E


Command Result : No Error


lunacm:>hsm init -label HSM10E -iped

        You are about to initialize the HSM.
        All contents of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error
```

```
lunacm:>slot list

        Slot Id ->              4
        Label ->                HSM10E
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK



        Current Slot Id: 4


Command Result : No Error


lunacm:>slot set -ss4

        Current Slot Id:    4     (Luna Admin Slot 7.7.2 (PED) Key Export With Cloning Mo
de)

Command Result : No Error


lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error


lunacm:>hsm changeHP -policy 12 vvalue 0

        You are about to change a destructive HSM policy.
        All partitions of the HSM will be destroyed.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

Command Result : No Error


lunacm:>hsm changeHP -policy 21 -value 0

Command Result : No Error
```

```
lunacm:>hsm showinfo

        Slot Id -> 4
        Partition Label -> HSM10E
        Partition Serial Number -> 712477
        Partition Model -> Luna G7
        Partition Manufacturer ->
        Partition Status -> L3 Device, OK
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   SO logged in
        RPV Initialized -> No

        Partition SMK OUIDs:
                SMK-FW4: Not Initialized
                SMK-FW6: Not Initialized
                SMK-FW7-FM: Not Initialized
                SMK-FW7-Rollover: Not Initialized
                SMK-FW7-Primary: 1e000000050000021ddf0a00


        Partition Storage:
                Total Storage Space:  655360
                Used Storage Space:   0
                Free Storage Space:   655360
                Object Count:         0
                Overhead:             24408

        System Times:
                HSM  : Fri Apr 26 20:06:49 UTC 2024
                Host : Fri Apr 26 20:06:49 UTC 2024
                Difference: 0 sec

        HSM Storage:
                Total Storage Space:  33554432
                Used Storage Space:   679768
                Free Storage Space:   32874664
                Allowed Partitions:   1
                Number of Partitions: 0

        HSM Part Number -> 808-000080-001

        Environmental:
                System Temperature :  38 deg. C

        Firmware Version -> 7.7.2
        Bootloader Version ->  1.6.0
        Rollback Firmware Version -> Not Available

        License Count:
                1. 621000186-000 G7 Base CUF with Real Certificate

        *** The HSM is in FIPS approved operation mode. ***

Command Result : No Error


lunacm:>partition create

Command Result : No Error


lunacm:>slot list

        Slot Id ->              3
        Label ->
        Serial Number ->        1658864473964
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM10E
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK



        Current Slot Id: 4

Command Result : No Error


lunacm:>slot set -s 3

        Current Slot Id:    3     (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error


lunacm:>partition init -label HSM10E_KSK-2024

        You are about to initialize the partition.

        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Please attend to the PED.

Command Result : No Error


lunacm:>role login -name po
```

```
        Please attend to the PED.

 Command Result : No Error


 lunacm:>partition changepolicy -policy 22 -value 1

 Command Result : No Error


 lunacm:>role init -name co

        Please attend to the PED.

 Command Result : No Error


 lunacm:>role createchallenge -name co

        Please attend to the PED.


        enter new challenge secret: ********


        re-enter new challenge secret: ********


 Command Result : No Error


 lunacm:>role logout

 Command Result : No Error


 lunacm:>role login -name co


        enter password: ********


        Please attend to the PED.

 Command Result : No Error


 lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM10E_KSK-2024
        Serial Number ->        1658864473964
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM10E
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 3


 Command Result : No Error


 lunacm:>partition archive list -slot 105

        HSM Storage Information for slot 105:

           Total HSM Storage Space: 33816576
           Used HSM Storage Space:  705868
           Free HSM Storage Space:  33110708
           Allowed Partitions:      100
           Number Of Partitions:    1

        Partition list for slot 105

           Number of partitions: 1

           Slot Id:                 5
           Label:                   KSK-2024
           Total Storage Size:      1884
           Used Storage Size:       1884
           Free Storage Size:       0
           Number Of Objects:       2

           Partition Cloning Version: 3
           Partition FM Status:        FM Disabled

           Partition SMK OUIDs:
                   SMK-FW4: Not Initialized
                   SMK-FW6: Not Initialized
                   SMK-FW7-FM: Not Initialized
                   SMK-FW7-Rollover: Not Initialized
                   SMK-FW7-Primary: Not Initialized


 Command Result : No Error


 lunacm:>partition archive contents -slot 105 partition KSK-2024
```

```
        Logging in as the user on slot 105.

        Please attend to the PED.

        Contents of partition KSK-2024 on slot 105 :

        Object list:

        Label:          Kmyv6jo
        Handle:         80
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         75
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00


        Number of objects:  2

Command Result : No Error

lunacm:>partition archive restore -slot 105 -partition KSK-2024

        Logging in to partition KSK-2024 on slot 105 as the user.

        Please attend to the PED.

        Verifying that all objects can be restored...

        2 objects will be restored.

        Restoring objects...
        Cloned object 80 from partition KSK-2024 (new handle 76).
        Cloned object 75 from partition KSK-2024 (new handle 79).

        Restore Successfully Completed.

        2 objects have been restored from partition KSK-2024 on slot 105.

Command Result : No Error

lunacm:>partitionoontents

        The 'Crypto Officer' is currently logged in. Looking for objects
        accessible to the 'Crypto Officer'.

        Object list:

        Label:          Kmyv6jo
        Handle:         79
        Object Type:    Private Key
        Usage Limit:    none
        Object UID:     3b0000000500000222df0a00

        Label:          Kmyv6jo
        Handle:         76
        Object Type:    Public Key
        Usage Limit:    none
        Object UID:     3a0000000500000222df0a00


        Number of objects:  2

Command Result : No Error


lunacm:>exit
k933[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# kskm-k\007eymaster --hsm luna invento
2023+0A026120:20:55,190: kskm.common.config: INFO Loaded configuration from file ksrsigne
r.yaml SHA-256 5a2ff2646e14ab6883fd972faf9baf1cd91c237a01df738b1f9288a6449ed3ec WORDS enl
ist combustion uproot getaway goldfish belowground rhythm gravity Mohawk Wyoming preshrun
k combustion rocker Norwegian rocker Brazilian sugar Brazilian blowtorch infancy absurd t
herapist hockey Medusa billiard misnomer newborn paragon crumpled onlooker stapler unicor
n
2024-04-26 20:20:55,226: kskm.common.config: INFO Configuration validated
2024-04-26 20:20:55,226: kskm.misc.hsm: INFO Initializing PKCS#11 module luna using /usr/
safenet/lunaclient/lib/libCryptoki2_64.so
2024-04-26 20:20:55,517: kskm.misc.hsm: INFO HSM First slot:       HSM10E_KSK-2024

2024-04-26 20:20:55,517: kskm.misc.hsm: INFO HSM ManufacturerID:

2024-04-26 20:20:55,517: kskm.misc.hsm: INFO HSM Model:            Luna G7
2024-04-26 20:20:55,517: kskm.misc.hsm: INFO HSM Serial:           1658864473964
2024-04-26 20:20:55,517: kskm.tools.keymaster: INFO Show HSM inventory
2024-04-26 20:20:55,526: kskm.tools.keymaster: INFO Key inventory:
HSM luna:
  Slot 3:
    Signing key pairs:
      Kmyv6jo alg=RSA bits=2048 exp=65537 -- Matching KSK not found in configuration
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# &d07md /media/HMSFD
b83B[?2d04/media/HMSFD: No such file or directory
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# /\00Ed /media/HMSB03[1R033[1P\033[1@S
\033[1@M
\033[?2004h(kskm) root@coen:/media/HSMFD# lanacm
1088¢m2064±bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->              3
        Label ->                HSM10E_KSK-2024
        Serial Number ->        1658864473964
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
Mode
        Slot Description ->     User Token Slot


        Slot Id ->              4
        Label ->                HSM10E
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 3

lunacm:>slot list

        Slot Id ->              3
        Label ->                HSM10E_KSK-2024
        Serial Number ->        1658864473964
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
Mode
        Slot Description ->     User Token Slot

        Slot Id ->              4
        Label ->                HSM10E
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Slot Id ->              105
        Label ->                BHSM2W
        Serial Number ->        718018
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Backup Mode
        Slot Description ->     Admin Token Slot
        HSM Status ->           L3 Device, OK


        Current Slot Id: 3

Command Result : No Error

lunacm:>slot set -s 105

        Current Slot Id:  105     (Luna Admin Slot 7.7.2 (PED) Backup Device)
```

```
Command Result : No Error

lunacm:>role login -name so

        Please attend to the PED.

Command Result : No Error

lunacm:>stm transport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: KJ5d-MFxP-LC46-MdpA


         Random User String: /L4S-GKJ7-qsG7-FJdP


Command Result : No Error


lunacm:>exit
\033[?2004h(kskm) root@coen:/media/HSMFD# echo BHSM2W
BHSM2W20041
\033[?2004h(kskm) root@coen:/media/HSMFD# screencap-verify
\033[?2004h(kskm) root@coen:/media/HSMFD# lunacm
\033cm2004±bit) v10.6.0-669. Copyright (c) 2023 Thales Group. All rights reserved.


        Available HSMs:

        Slot Id ->              3
        Label ->                HSM10E_KSK-2024
        Serial Number ->        1658864473964
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna User Partition With SO (PED) Key Export With Cloning
Mode
        Slot Description ->     User Token Slot

        Slot Id ->              4
        Label ->                HSM10E
        Serial Number ->        712477
        Model ->                Luna G7
        Firmware Version ->     7.7.2
        Bootloader Version ->   1.6.0
        Configuration ->        Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
```

```
        Slot Description ->      Admin Token Slot
        HSM Status ->            L3 Device, OK


        Current Slot Id: 3

lunacm:>slot list

        Slot Id ->               3
        Label ->                 HSM10E_KSK-2024
        Serial Number ->         1658864473964
        Model ->                 Luna G7
        Firmware Version ->      7.7.2
        Bootloader Version ->    1.6.0
        Configuration ->         Luna User Partition With SO (PED) Key Export With Cloning
 Mode
        Slot Description ->      User Token Slot


        Slot Id ->               4
        Label ->                 HSM10E
        Serial Number ->         712477
        Model ->                 Luna G7
        Firmware Version ->      7.7.2
        Bootloader Version ->    1.6.0
        Configuration ->         Luna HSM Admin Partition (PED) Key Export With Cloning Mo
de
        Slot Description ->      Admin Token Slot
        HSM Status ->            L3 Device, OK


        Current Slot Id: 3

Command Result : No Error

lunacm:>slot set -s 23

        Current Slot Id:    3     (Luna User Slot 7.7.2 (PED) Key Export With Cloning Mod
e)

Command Result : No Error

lunacm:>role deactivate naame co

Command Result : No Error

lunacm:>slot set -s 4

        Current Slot Id:    4     (Luna Admin Slot 7.7.2 (PED) Key Export With Cloning Mo
de)

Command Result : No Error

lunacm:>role login -name so

        Please attend to the PED.
```

```
Command Result : No Error

lunacm:>stmttrassport

        You are about to configure the HSM in STM.
        Are you sure you wish to continue?

        Type 'proceed' to continue, or 'quit' to quit now ->proceed

        Configuring the HSM for transport (may take up to 3 minutes)...

        HSM was successfully configured for transport.

        Please record the displayed verification & random user strings.
        These are required to recover from Secure Transport Mode.


        Verification String: TXAM-46FJ-EWsP-qR6/


         Random User String: NJEX-ECMJ-EHqt-dJdq


Command Result : No Error


lunacm:>exit
\033[?2004h(kskm) root@coen:/media/HSMFD# echo HSM10E
HSM10E20041
\033[?2004h(kskm) root@coen:/media/HSMFD# screenappvverify
\033[?2004h(kskm) root@coen:/media/HSMFD# exit
\033[?20041

Script done on 2024-04-26 20:51:34+00:00 [COMMAND_EXIT_CODE="0"]
```

# Act 4: Secure Hardware

The CA will secure the ceremony hardware to prepare it for storage by performing the steps below:

- Copy the HSMFD contents
- Print log information
- Place the equipment and Crypto Officer credentials inside of TEBs
- Along with IW, escort SSC1 and equipment cart into Tier 5 (Safe Room) to return equipment to Safe #1
- Along with IW, escort SSC2 and COs into Tier 5 (Safe Room) to place Crypto Officers' credentials to Safe #2

## Stop logging the Terminal Session

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.1 | CA performs the following steps to stop logging:<br>a) Execute the command below using the **Commands** terminal window to stop logging the terminal session:<br>`exit` ✓<br>**Note: The Commands terminal session window will remain open.**<br>b) Disconnect the USB HSM cables from the laptop. ✓ | Y.Y. | 20:51 |

## Print Logging Information

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.2 | CA executes the following commands to print a copy of the logging information:<br>`print-script script-202404*.log`<br>Attach the printed copies to IW script.<br>**Note: Ignore the error regarding non-printable characters if prompted.** | Y.Y. | 20:54 |

## Prepare Blank FDs and Copy the HSMFD Contents

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.3 | CA executes the following command **twice** to print **four** copies of the hash for the HSMFD content:<br>`hsmfd-hash -p` ✓✓<br>**Note: One copy for HSMFD bundle, one copy for each audit bundle, and one copy for the OS media TEB.** | Y.Y. | 20:55 |
| 4.4 | CA executes the command below to display the contents of the HSMFD:<br>`ls -ltrR` ✓ | Y.Y. | 20:56 |
| 4.5 | CA executes the command below and follows the interactive prompts in the terminal window to create **seven** HSMFDs copies:<br>`copy-hsmfd` ✓ 卌 \|\|<br>**Note 1: Wait for the activity light on the copied HSMFD to stop flashing before removal.**<br>**Note 2: "copy-hsmfd -v" can be used to activate verbose mode.** | Y.Y. | 21:03 |

## Place HSMFDs and OS Media into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.6 | Using the **Commands** terminal window, CA executes the commands below to unmount the HSMFD:<br>a) `cd /tmp` ✓<br>b) `umount /media/HSMFD` ✓<br>CA removes the HSMFD, then places it on the holder. ✓<br>**Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.** | Y.Y. | 21:03 |
| 4.7 | CA performs the following steps to shut down the laptop:<br>a) Power **OFF** the laptop by pressing the power button. ✓<br>b) Disconnect all connections from the laptop. ✓<br>c) Remove the OS media from the laptop, and place it in its case. ✓<br>d) Close all laptop latches. ✓ | Y.Y. | 21:04 |
| 4.8 | CA performs the following steps to prepare the OS media bundle for storage:<br>a) Ask the IW for the OS media bundle's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>b) Place 2 HSMFDs and 2 OS media SD cards into a plastic card case. ✓<br>c) Place the plastic card case containing 2 HSMFDs and 2 OS media SD cards along with 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seal it. ✓<br>d) Give IW the sealing strips for post-ceremony inventory. ✓<br>e) Place the OS media bundle onto the HSM designated space of the ceremony table visible to the audit camera. ✓<br>f) Initial the TEB along with IW using a ballpoint pen. ✓<br>g) Place the OS media bundle TEB on the cart. ✓<br>**OS Media (release coen-1.1.0) + HSMFD: TEB # BB02639625** ✓ | Y.Y. | 21:07 |
| 4.9 | CA performs the following steps to prepare the KMF-West HSMFD bundle for transport:<br>a) Ask the IW for the HSMFD bundle's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>b) Place 2 HSMFDS into a plastic card case. ✓<br>c) Place the plastic card case containing 2 HSMFDs and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seal it. ✓<br>d) Give IW the sealing strips for post-ceremony inventory. ✓<br>e) Place the HSMFD bundle onto the HSM designated space of the ceremony table visible to the audit camera. ✓<br>f) Initial the TEB along with IW using a ballpoint pen. ✓<br>g) Call RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. ✓<br>h) Give RKOS the TEB. ✓<br>**KMF West Transport HSMFD TEB # BB02639627** ✓ | Y.Y. | 21:09 |
| 4.10 | CA distributes the following HSMFDs:<br>2 for IW (for audit bundles). ✓<br>2 for RKOS (for SKR exchange with RZM and process review). ✓ | Y.Y. | 21:09 |

## Place Laptop4 into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.11 | CA performs the following steps to prepare the Laptop for storage:<br>a) Ask the IW for the Laptop's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. ✓<br>b) Read aloud the service tag number from the bottom of the laptop while the IW verifies it matches the information below. ✓<br>c) Place the Laptop into its designated new TEB, then seal it. ✓<br>d) Give IW the sealing strips for post-ceremony inventory. ✓<br>e) Place the Laptop onto the HSM designated space of the ceremony table visible to the audit camera. ✓<br>f) Initial the TEB along with IW using a ballpoint pen. ✓<br>g) Place the Laptop TEB on the cart. ✓<br>**Laptop4: TEB # BB81420050 ✓ / Service Tag # 58SVSG2 ✓** | Y.Y. | 21:11 |

## Place Crypto Officers' Credentials into TEBs

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.12 | The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps:<br>a) CA asks the IW for the CO's designated new **CO** and **SO** TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. ✓✓✓✓✓✓✓<br>b) CA gives the designated plastic credential case to CO and they take their **CO** and **SO** iKeys from the credential stand and place them in the case, then returns it to CA. ✓✓✓✓✓✓✓<br>c) CA along with IW inspects the designated plastic credential case to ensure it contains the **CO** and **SO** iKeys allocated to the CO. ✓✓✓✓✓✓✓<br>d) CA places the plastic case into its designated new TEB, then seals it. ✓✓✓✓✓✓✓<br>e) CA gives the IW sealing strips for post-ceremony inventory. ✓✓✓✓✓✓✓<br>f) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. ✓✓✓✓✓✓✓<br>g) CA initials the TEB with a ballpoint pen. ✓✓✓✓✓✓✓<br>h) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. ✓✓✓✓✓✓✓<br>i) Repeat steps **a) to h)** for the **Audit** and **Domain** TEB and iKeys.<br>j) CO inspects the TEBs, verifies their contents, then initials both with a ballpoint pen. ✓✓✓✓✓✓✓<br>k) CO writes the date and time, signs the credential table of the IW's script, then IW initials the entry. ✓✓✓✓✓✓✓<br>l) CO returns to their seat with their TEBs. ✓✓✓✓✓✓✓<br>m) Repeat steps for all the remaining COs on the list. ✓<br><br>**Crypto Officer 1: Frederico Neves**<br>**CO and SO TEB # BB02639650** ✓<br>**Audit and Domain TEB # BB02639649** ✓<br><br>**Crypto Officer 2: Pia Gruvö**<br>**CO and SO TEB # BB02639648** ✓<br>**Audit and Domain TEB # BB02639647** ✓<br><br>**Crypto Officer 3: Ondrej Filip**<br>**CO and SO TEB # BB02639646** ✓<br>**Audit and Domain TEB # BB02639645** ✓<br><br>**Crypto Officer 4: Robert Seastrom**<br>**CO and SO TEB # BB02639644** ✓<br>**Audit and Domain TEB # BB02639643** ✓<br><br>**Crypto Officer 5: Nomsa Mwayenga**<br>**CO and SO TEB # BB02639642** ✓<br>**Audit and Domain TEB # BB02639641** ✓<br><br>**Crypto Officer 6: Hugo Salgado**<br>**CO and SO TEB # BB02639640** ✓<br>**Audit and Domain TEB # BB02639639** ✓<br><br>**Crypto Officer 7: Dileepa Lathsara**<br>**CO and SO TEB # BB02639638** ✓<br>**Audit and Domain TEB # BB02639637** ✓ | Y.Y. | 21:39 |

| TCR | TEB # | Printed Name | Signature | Date | Time | IW Initials |
|---|---|---|---|---|---|---|
| **CO1** | CO and SO TEB #<br>**BB02639650**<br>Audit and Domain TEB #<br>**BB02639649** | **Frederico Neves** | Frederico Neves | **2024 Apr** 26 | 2118 | Y.Y. |
| **CO2** | CO and SO TEB #<br>**BB02639648**<br>Audit and Domain TEB #<br>**BB02639647** | **Pia Gruvö** |  | **2024 Apr** 26 | 21:21 | Y.Y. |
| **CO3** | CO and SO TEB #<br>**BB02639646**<br>Audit and Domain TEB #<br>**BB02639645** | **Ondrej Filip** | Ondřej Filip | **2024 Apr** 26 | 21:25 | Y.Y. |
| **CO4** | CO and SO TEB #<br>**BB02639644**<br>Audit and Domain TEB #<br>**BB02639643** | **Robert Seastrom** |  | **2024 Apr** 26 | 2128 | Y.Y. |
| **CO5** | CO and SO TEB #<br>**BB02639642**<br>Audit and Domain TEB #<br>**BB02639641** | **Nomsa Mwayenga** |  | **2024 Apr** 26 | 21:32 | Y.Y. |
| **CO6** | CO and SO TEB #<br>**BB02639640**<br>Audit and Domain TEB #<br>**BB02639639** | **Hugo Salgado** |  | **2024 Apr** 26 | 21:35 | Y.Y. |
| **CO7** | CO and SO TEB #<br>**BB02639638**<br>Audit and Domain TEB #<br>**BB02639637** | **Dileepa Lathsara** |  | **2024 Apr**26 | 21.38 | Y.Y. |

## Return the Equipment to Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.13 | CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.) | Y.Y. | 21:40 |
| 4.14 | SSC1 opens Safe #1 while shielding the combination from the camera.<br>**Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.** | Y.Y. | 21:41 |
| 4.15 | SSC1 removes the safe log, writes the date and time, then signs the safe log where **"Open Safe"** is indicated.<br>IW verifies this entry, then initials it.<br>**Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** | Y.Y. | 21:41 |
| 4.16 | CA performs the following steps to return each piece of equipment to the safe:<br>a) CAREFULLY remove the equipment TEB from the cart.<br>b) Read aloud the TEB number, then verify its integrity.<br>c) Present the equipment TEB to the audit camera above, then place it inside Safe #1 (Equipment Safe).<br>d) Write the date, time, and signature on the safe log where **"Return"** is indicated.<br>e) IW verifies the safe log entry, then initials it.<br>**HSM9E: TEB # BB02639624** ✓<br>**BHSM1E: TEB # BB02639622** ✓<br>**BHSM2E: TEB # BB02639621** ✓<br>**HSM10E: TEB # BB02639623** ✓<br>**Laptop4: TEB # BB81420050** ✓<br>**OS media (release coen-1.1.0) + HSMFD: TEB # BB02639625** ✓<br>**Note: The shelves in the equipment safe can slide in and out for ease of use.** | Y.Y. | 21:45 |

## Close Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.17 | SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it. | Y.Y. | 21:45 |
| 4.18 | SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, then ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator adjacent to the Tier 5 (Safe Room) exit door is off. | Y.Y. | 21:46 |
| 4.19 | CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room). | Y.Y. | 21:46 |

## Open Safe #2 (Tier 6, Credentials Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.20 | CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.) | Y.Y. | 21:48 |
| 4.21 | SSC2 opens Safe #2 while shielding the combination from the camera.<br>**Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.** | Y.Y | 21:49 |
| 4.22 | SSC2 removes the safe log, writes the date and time, then signs the safe log where **"Open Safe"** is indicated.<br>IW verifies this entry, then initials it.<br>**Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** | Y.Y | 21:50 |

## COs Place the Credentials to Safe Deposit Boxes (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4.23 | COs perform the following steps sequentially to place the listed TEBs:<br>a) CO reads aloud the TEB number, verifies integrity of TEB, then presents it to the audit camera above.<br>b) CO announces their box number, then CA operates the guard key in that box's lower lock with the key blade facing downward.<br>c) CO operates their tenant key in that box's upper lock with the key blade facing upward, then opens the safe deposit box.<br>d) CO places their TEB(s) in their safe deposit box, locks it, then removes their key.<br>e) CO writes the date and time, then signs the safe log where **"Place"** is indicated.<br>f) IW verifies the completed safe log entry, then initials it.<br>g) CA locks the safe deposit box, then removes the guard key.<br><br>**Crypto Officer 1: Frederico Neves**<br>**Safe Deposit Box # 1239**<br>**CO and SO TEB # BB02639650** ✓<br>**Audit and Domain TEB # BB02639649** ✓<br><br>**Crypto Officer 2: Pia Gruvö**<br>**Safe Deposit Box # 1264**<br>**CO and SO TEB # BB02639648** ✓<br>**Audit and Domain TEB # BB02639647** ✓<br><br>**Crypto Officer 3: Ondrej Filip**<br>**Safe Deposit Box # 1241**<br>**CO and SO TEB # BB02639646** ✓<br>**Audit and Domain TEB # BB02639645** ✓<br><br>**Crypto Officer 4: Robert Seastrom**<br>**Safe Deposit Box # 1243**<br>**CO and SO TEB # BB02639644** ✓<br>**Audit and Domain TEB # BB02639643** ✓<br><br>**Crypto Officer 5: Nomsa Mwayenga**<br>**Safe Deposit Box # 1262**<br>**CO and SO TEB # BB02639642** ✓<br>**Audit and Domain TEB # BB02639641** ✓<br><br>**Crypto Officer 6: Hugo Salgado**<br>**Safe Deposit Box # 1242**<br>**CO and SO TEB # BB02639640** ✓<br>**Audit and Domain TEB # BB02639639** ✓<br><br>**Crypto Officer 7: Dileepa Lathsara**<br>**Safe Deposit Box # 1263**<br>**CO and SO TEB # BB02639638** ✓<br>**Audit and Domain TEB # BB02639637** ✓ | Y.Y. | 22:08 |

## Close Safe #2 (Tier 6, Credentials Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| **4.24** | Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry, then initials it. | Y.Y. | 22:04 |
| **4.25** | SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, then ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator adjacent to the Tier 5 (Safe Room) exit door is off. | Y.Y. | 22:04 |
| **4.26** | CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room). | Y.Y. | 22:05 |

# Act 5: Close the Key Signing Ceremony

The CA will finish the ceremony by performing the following steps:

- Read any exceptions that occurred during the ceremony
- Call the ceremony participants to sign the IW's script
- Stop the online streaming and video recording

## Participants Sign IW's Script

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5.1 | CA reads all exceptions that occurred during the ceremony. | Y.Y | 22:08 |
| 5.2 | CA calls each in-person attendee not seated at the ceremony table to sign the IW's participant list. **All signatories declare to the best of their knowledge that this script is a true and accurate record of the ceremony.**<br>All in-person attendees may sign to attest the **Root KSK 2024** generation output log. | Y.Y. | 22:16 |
| 5.3 | CA reviews IW's script, then signs the participants list. | Y.Y. | 22:20 |
| 5.4 | IW signs the list and records the completion time. | Y.Y. | 22:21 |

## Stop Online Streaming and Recording

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5.5 | CA acknowledges the participation of the online participants, then instructs the SA to stop the online streaming. | Y.Y. | 22:25 |
| 5.6 | CA instructs the SA to stop the audit camera video recording. | Y.Y. | 22:25 |
| 5.7 | CA informs onsite participants of post ceremony activities. | Y.Y | 22:26 |
| 5.8 | Ceremony participants take a group photo. | Y.Y | 22:26 |

# Appendix A: Glossary

[1] **COEN:** The Ceremony Operating ENvironment (COEN) is a Reproducible ISO image consisting of a live operating system. More information and the OS image source code can be found at:

https://github.com/iana-org/coen

[2] **configure-printer:*** A bash script used to install the HP LaserJet print driver from the command line instead of **system-config-printer**.

[3] **copy-hsmfd:*** A bash script used to copy HSMFD contents to new flash drives; includes verification via hash comparison.

[4] **hsmfd-hash:*** A bash script used to calculate, print, and compare SHA-256 checksums for the HSMFD flash drives.

**Note: The sort command has different behavior depending on the locale settings specified by environment variables. Current OS locale setting is** `LC_COLLATE="POSIX"`

[5] **kskm-keymaster:**** An application that creates and deletes keys and performs a key inventory.

[6] **kskm-ksrsigner:**** An application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.

[7] **ksrsigner:** A legacy application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.

The source code is available at https://github.com/iana-org/dnssec-keytools-legacy

[8] **ping hsm:** The HSM static IP address **192.168.0.2** has been included in the **/etc/hosts** file.

[9] **printlog:*** A bash script used to print the Key Signing Log output from **ksrsigner** application.

[10] **print-script:*** A bash script used to print the terminal commands.

[11] **print-ttyaudit:*** A bash script used to print the HSM logs.

[12] **sha2wordlist:** An application that reads data from STDIN and outputs a SHA-256 checksum as hex and PGP words in STDOUT.

The source code is available at https://github.com/kirei/sha2wordlist

[13] **ttyaudit:*** A perl script used to capture and log the HSM output.

* The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-1.1.0coen_amd64.deb
A debian package is an **ar** archive. To extract data from a deb package, use the command **ar -x ksk-tools-1.1.0coen_amd64.deb**
Then extract the files with **tar -xvf data.tar.xz**
The file will be located in the directory: **./opt/icann/bin/**

** The source code is available at https://github.com/iana-org/dnssec-keytools

[14] **Keyper HSM Role Cards:**

a) **OP (Operator):** Configures the HSM to an online or offline state toggling communication through its ethernet adapter. Required for communication with the laptop for key signing operations.

b) **SO (Security Officer):** Used for HSM administrative operations. Required to create other role cards (OP and CO), and the introduction or zeroization of an HSM.

c) **CO (Crypto Officer):** Used for the key management functions in an HSM. Required for adding or deleting keys stored in an HSM.

d) **SMK (Storage Master Key):** Allows an HSM to read an encrypted APP key (KSK) backup. Required for initial migration of keys and disaster recovery.

e) **AAK (Adapter Authorization Key):** Configures an HSM to use previously generated OP, CO, and SO cards. Required for the introduction of an HSM.

f) **APP (Application Key):** An encrypted backup copy of one or more keys stored in an HSM, which can only be decoded by its corresponding SMK. Required for migrating keys and disaster recovery.

[15] **Thales Luna HSM Role iKeys:**

a) **CO (Crypto Officer):** Used for the key management functions in the HSM. Required for adding or deleting keys stored in an HSM.

b) **SO (Security Officer):** Required for administration of the HSMs.

c) **Audit:** Required to access transaction logs from the HSMs.

d) **Domain:** Associates HSMs to facilitate cloning key materials to dedicated Luna backup HSMs.

# Appendix B: Audit Bundle Checklist

## 1. Output of Signer System (by CA)

Each audit bundle will contain one HSMFD. All bundles will be placed inside TEBs that are pre-labeled Audit Original and Audit Copy

## 2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes generated during the ceremony, and attestation. See Appendix C on page 96.

## 3. Audio-Visual Recordings from the KSK Ceremony (by SA)

Two sets of the audit camera footage - One for the original audit bundle and the other for the duplicate audit bundle.

## 4. Logs from the Physical Access Control System and Intrusion Detection System (by SA)

Two electronic copies of the following:

1. Firewall configuration
2. Configuration reports
3. Personnel/cardholder reports
4. Activity and audit log reports

These files will be placed inside two separate Flash Drives that are labeled "Audit".

The contents of the Flash Drive will be confirmed by the IW before placing each of them inside the original and the duplicate audit bundles.

## 5. Configuration review of the Physical Access Control System and Intrusion Detection System (by SA)

SA's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix D on page 97.

## 6. Configuration review of the Firewall System (by SA)

SA's attestation and hard copies of the firewall configuration from the review process. See Appendix E on page 98. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

## 7. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 53-2**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

# Appendix C: Key Ceremony Script (by IW)

I hereby attest that the Key Ceremony was conducted in accordance with this script. Any exceptions that occurred were accurately and properly documented.

IW: **Yuko Yokoyama**

Signature: ______________________

Date: 2024 Apr 26

# Appendix D: Access Control System Configuration Review (by SA)

In my review of the KMF's Access Control System, I attest that the following are true and correct to the best of my knowledge:

a) There were NO discrepancies found in the system configurations, assigned authorizations, and audit logs.

b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

Below are the reports that were generated from the access control system:

1. List of Personnel with assigned Access Group.
2. Configuration of Areas and Access Groups.
3. Logs for Access Event activities and Configuration activities.

Range: **20240425 00:00:00 to 20240427 00:00:00 UTC.**

SA: Reed Quinn

Signature:

Date: 2024 Apr 26

# Appendix E: Firewall Configuration Review (by SA)

I have reviewed and confirmed that the firewall configuration satisfies the requirements of the DNSSEC Practice Statement with version 7th Edition (2024-03-15). No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA: Reed Quinn

Signature:

Date: 2024 Apr26