

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 | CA = Ceremony Administrator | CO = Crypto Officer |
| EW = External Witness | FD = Flash Drive | HSM = Hardware Security Module |
| IW = Internal Witness | KMF = Key Management Facility | KSR = Key Signing Request |
| MC = Master of Ceremonies | OP = Operator | PTI = Public Technical Identifiers |
| RKSH = Recovery Key Share Holder | RKOS = RZ KSK Operations Security | RZM = Root Zone Maintainer |
| SA = System Administrator | SKR = Signed Key Response | SMK = Storage Master Key |
| SO = Security Officer | SSC = Safe Security Controller | STM = Secure Transport Mode |
| SW = Staff Witness | TCR = Trusted Community Representative | |
| 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 —	
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			
SA	Reed Quinn / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Kim Davies / PTI			
EW	Ólafur Guðmundsson / CO5 West			

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.		
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.		
1.3	CA asks that any first-time ceremony participants in the room introduce themselves.		

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
1.4	CA reviews emergency evacuation procedures with onsite participants.		
1.5	CA explains the use of personal electronic devices during the ceremony.		
1.6	CA summarizes the purpose of the ceremony.		

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): Date and time: _____ Note: All entries into this script or any logs should follow this common source of time.		

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.)		
1.9	SSC1 opens Safe #1 while shielding the combination from the camera. 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.		
1.10	Perform the following steps to update the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry, then initials it.		

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

Step	Activity	Initials	Time
1.11	<p>CA performs the indicated action for each item listed below with the following steps:</p> <ul style="list-style-type: none"> a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud the TEB number, verify its integrity, then present it to the audit camera above. c) Place the equipment TEB on the cart as specified in the list below. d) Write the date and time, then sign the safe log. e) IW verifies the completed safe log entries, then initials them. <p>HSM9E: TEB # BB02638477 (Place on Cart) Last Verified: AT Ceremony 53-2 2024-03-27</p> <p>BHSM1E: TEB # BB02638476 (Place on Cart) Last Verified: AT Ceremony 53-2 2024-03-27</p> <p>BHSM2E: TEB # BB02638475 (Place on Cart) Last Verified: AT Ceremony 53-2 2024-03-27</p> <p>BHSM1W: TEB # BB02638474 (Place on Cart) Last Verified: AT Ceremony 53-2 2024-03-27</p> <p>BHSM2W: TEB # BB02638473 (Place on Cart) Last Verified: AT Ceremony 53-2 2024-03-27</p> <p>HSM10E: TEB # BB02638472 (Place on Cart) Last Verified: AT Ceremony 53-2 2024-03-27</p> <p>Laptop4: TEB # BB81420078 (Place on Cart) Last Verified: KSK Ceremony 51 2023-11-30</p> <p>OS media (release coen-1.1.0) + HSMFD: TEB # BB02639666 (Place on Cart) Last Verified: KSK Ceremony 53-1 2024-04-25</p> <p>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. The shelves in the equipment safe can slide in and out for ease of use.</p>		

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.		
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.		
1.14	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		

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	<p>CA performs the following steps to prepare each item listed below:</p> <ol style="list-style-type: none"> a) Remove the TEB from the cart, then place it on the ceremony table. b) Inspect the equipment TEB for tamper evidence. 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. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. <p>Laptop4: TEB # BB81420078 / Service Tag # 58SVSG2 Last Verified: KSK Ceremony 51 2023-11-30 OS media (release coen-1.1.0) + HSMFD: TEB # BB02639666 Last Verified: KSK Ceremony 53-1 2024-04-25</p> <p>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.</p>		
2.2	<p>CA performs the following steps to confirm that no hard drive and battery are in the laptop:</p> <ol style="list-style-type: none"> a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty. 		
2.3	<p>CA ensures the lock switch on the left side of the listed SD card is slid down to the lock position: OS media release coen-1.1.0 Copy # 2</p>		
2.4	<p>CA performs the following steps to boot the laptop:</p> <ol style="list-style-type: none"> a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect two USB HSM cables into the right-side USB ports of the laptop. c) Connect the external HDMI display cable into the left-side HDMI port of the laptop. d) Connect the power supply into the back of the laptop toward the CA'S left side. e) Insert the OS media release coen-1.1.0 Copy # 2 into the right-side of the laptop. f) Switch it ON. 		
2.5	<p>CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the View menu and select Zoom In or Zoom Out To change the resolution of each screen: Go to Applications > Settings > Display</p>		

Invert the Terminal Text and Background Colors

Step	Activity	Initials	Time
2.6	<p>CA performs the following steps to invert the text and background colors in the terminal:</p> <ol style="list-style-type: none"> Click the "Edit" menu, and select "Preferences..." Click on the "Colors" tab at the top of the preferences menu. Click the drop down arrow on the "Presets" menu, then select "Black on White". Close the Terminal Preferences window. <p>Note: The colors are being inverted for optimized printouts.</p>		

OS Media coen-1.1.0 Checksum Verification

Step	Activity	Initials	Time
2.7	<p>Using the Commands terminal window, CA executes the following steps:</p> <ol style="list-style-type: none"> Verify the byte count of the SD card matches the ISO size by running the following command: <code>df -B1 /dev/sda</code> Calculate the SHA-256 hash by executing: <code>head -c 602406912 /dev/sda sha2wordlist</code> IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. <p>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.</p> <p>SHA-256 hash: 2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8</p> <p>PGP Words: 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</p> <p>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</p>		

Printer Setup

Step	Activity	Initials	Time
2.8	CA confirms that the printer is switched ON:		
2.9	<p>Using the Commands terminal window, CA executes the command below to configure the printer and print a test page:</p> <p><code>configure-printer</code></p>		

Date Setup

Step	Activity	Initials	Time
2.10	<p>Using the Commands terminal window, CA executes the command below to verify the date/time reasonably matches the ceremony clock.</p> <p><code>date</code></p> <p>If the date/time do not match, perform the following steps:</p> <ol style="list-style-type: none"> Execute <code>date -s "20240426 HH:MM:SS"</code> to set the time. where HH is two-digit hour, MM is two-digit minutes and SS is two-digit seconds. Execute <code>date</code> to confirm the date/time matches the clock. 		

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: a) Wait for the file system window to appear. b) Display the HSMFD contents to all participants. c) Close the file system window.		
2.12	Using the Commands terminal window, CA executes the command below to calculate the SHA-256 hash of the HSMFD: <code>hsmfd-hash -c</code> 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.		

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.		

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: <code>cd /media/HSMFD</code>		
2.15	Using the Commands terminal window, CA executes the command below to log activities of the terminal window: <code>script script-20240426.log</code>		

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: <code>mkdir HSM9E BHSM1E BHSM2E BHSM1W BHSM2W HSM10E</code>		

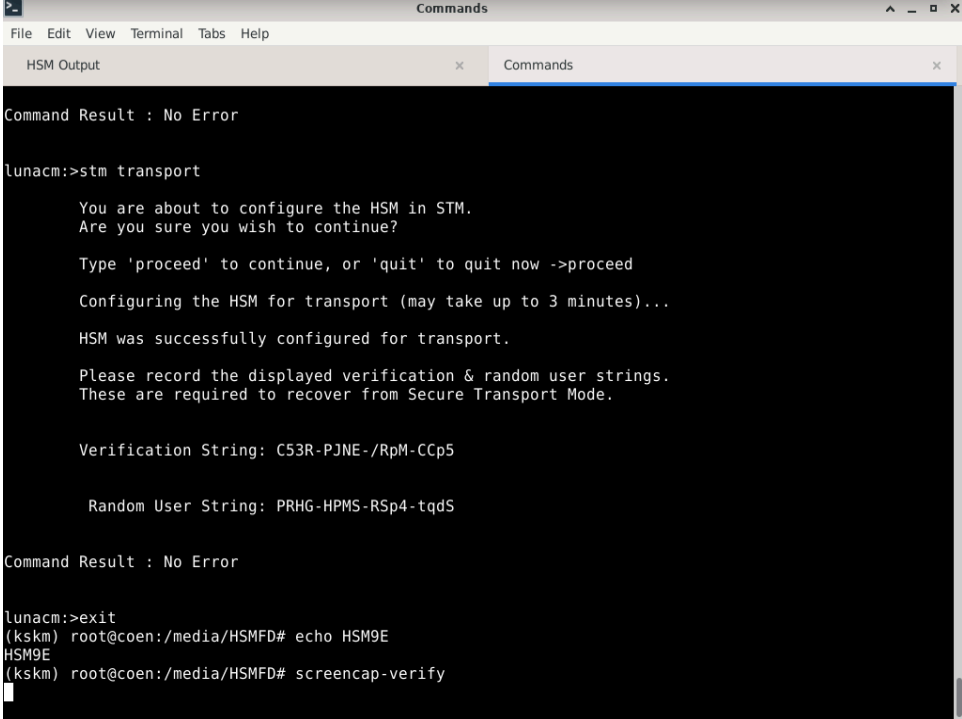
HSM9E (Tier 7) Setup

Step	Activity	Initials	Time
3.2	<p>CA performs the following steps to prepare HSM9E:</p> <ol style="list-style-type: none"> a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. 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. e) Read aloud the HSM9E serial number while IW verifies the information using the previous ceremony script where it was last used. f) Flip HSM9E over face up in its designated stand. <p>HSM9E: TEB # BB02638477 / Serial # 712482 Last Verified: AT Ceremony 53-2 2024-03-27</p>		

Power ON HSM9E (Tier 7)

Step	Activity	Initials	Time
3.3	<p>CA performs the following steps to prepare HSM9E:</p> <ol style="list-style-type: none"> a) Plug a USB HSM cable into the USB-C port on the top of HSM9E. b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. c) Wait for HSM9E to boot and confirm the device is in Secure Transport Mode (STM). d) Verify the displayed HSM serial number on the screen matches 712482. <p>HSM9E: Serial # 712482</p>		

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

Step	Activity	Initials	Time
<p>3.4</p>	<p>Using the Commands terminal window, CA executes the following steps to recover the HSM from STM:</p> <ol style="list-style-type: none"> Launch the LunaCM application: lunacm 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.  <p>Screenshot of HSM9E STM placement during AT Ceremony 53-2 2024-03-27</p> <ol style="list-style-type: none"> 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 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. 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 Once the string is verified type proceed, then press enter to recover HSM9E from STM. 		

Generate HSM9E (Tier 7) Audit Credentials

Step	Activity	Initials	Time
3.5	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> a) Initialize the audit role: <code>role init -name au</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the HSM9E touchscreen to generate a 3 of 7 audit credential set: Note: If the HSM9E touchscreen is off, tap it once to activate the display. d) When "Register your Auditor..." is displayed, select "Create new quorum of iKeys", then press continue. e) When "How many iKeys will make up the full Auditor?" is displayed, enter 7, then press the ✓ in the lower right corner. f) When "How many iKeys will be required for authentication?" is displayed, enter 3, then press the ✓ in the lower right corner. g) When "Please insert first iKey" is displayed, insert the first iKey in the audit set, then press continue. h) When "Create a new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. i) When "Re-enter your new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. j) When "First iKey successfully registered" is displayed, remove the iKey, then press continue. k) Repeat steps g) to j) for the 2nd, 3rd, 4th, 5th, 6th, and 7th audit iKeys. l) When "Registration successful" is displayed, press continue. <p>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 92.</p>		

Configure HSM9E (Tier 7) Audit Settings

Step	Activity	Initials	Time
3.6	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> Log in with the audit role: <code>role login -name au</code> Follow the instructions on the HSM9E touchscreen to perform audit authentication: Note: If the HSM9E touchscreen is off, tap it once to activate the display. When "Please ensure an iKey is inserted" is displayed, insert a randomly selected audit iKey, then press continue. When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When HSM9E returns to its dashboard, remove the last iKey of the audit set. Using the LunaCM terminal, synchronize the HSM's clock with the host time: <code>audit time sync</code> Set the filepath where log files are written: <code>audit config path /media/HSMFD/HSM9E</code> Set audit logging configuration: <code>audit config evmask all,failure,success</code> Type <code>proceed</code>, then press enter to continue. Set audit logging rotation interval: <code>audit config interval hourly@00</code> Set audit logging maximum log file size: <code>audit config size 4096k</code> Show the audit logging configuration: <code>audit config get</code> Confirm with IW the output of the logging configuration matches with the list below: <pre> 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 </pre> <p>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 92.</p>		

Initialize HSM9E (Tier 7) Administrative Partition

Step	Activity	Initials	Time
3.7	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the HSM9E administrative partition: <code>hsm init -label HSM9E -iped</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the HSM9E touchscreen to generate a 3 of 7 SO and 5 of 7 domain credential set: Note: If the HSM9E touchscreen is off, tap it once to activate the display. d) When "Register your Security Officer..." is displayed, select "Create new Quorum of iKeys", then press continue. e) When "How many iKeys will make up the full Security Officer?" is displayed, enter 7, then press the ✓ in the lower right corner. f) When "How many iKeys will be required for authentication?" is displayed, enter 3, then press the ✓ in the lower right corner. g) When "Please insert first iKey" is displayed, insert the first SO iKey, then press continue. h) When "Create a new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. i) When "Re-enter your new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. j) When "First iKey successfully registered" is displayed, remove the iKey, then press continue. k) Repeat steps g) to j) for the 2nd, 3rd, 4th, 5th, 6th, and 7th SO iKeys. l) When "Registration successful" is displayed, press continue to automatically initiate SO authentication. m) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. p) When "Set up your domain..." is displayed, remove the previous iKey, select "Create new domain", then press continue. q) When "How many iKeys will make up the full Domain?" is displayed, enter 7, then press the ✓ in the lower right corner. r) When "How many iKeys will be required for authentication?" is displayed, enter 5, then press the ✓ in the lower right corner. s) When "Please insert first iKey" is displayed, insert the first domain iKey, then press continue. t) When "Create a new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. u) When "Re-enter your new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. v) When "First iKey successfully set up" is displayed, remove the iKey, then press continue. w) Repeat steps s) to v) for the 2nd, 3rd, 4th, 5th, 6th, and 7th domain iKeys. x) When "Creation successful" is displayed, press finish. <p>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 92.</p>		

Configure HSM9E (Tier 7) Global Policies

Step	Activity	Initials	Time
3.8	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the HSM9E admin partition slot number: <code>slot list</code> b) Select the HSM9E admin partition slot: <code>slot set -s 4</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the HSM9E touchscreen to perform SO authentication: Note: If the HSM9E touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When HSM9E returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, activate FIPS mode: <code>hsm changeHP -policy 12 -value 0</code> j) Type <code>proceed</code>, then press enter to continue. k) Disable PIN change after setup: <code>hsm changeHP -policy 21 -value 0</code> l) Verify HSM9E is in FIPS approved operation mode: <code>hsm showinfo</code> <p>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 92.</p>		

Create HSM9E (Tier 7) Application Partition

Step	Activity	Initials	Time
3.9	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Create the partition: <code>partition create</code> b) Verify the application partition slot number: <code>slot list</code> c) Select the application partition slot: <code>slot set -s 3</code> d) Initialize the application partition: <code>partition init -label HSM9E_KSK-2024</code> e) Type proceed, then press enter to continue. f) Follow the instructions on the HSM9E touchscreen to register the SO and domain credential sets: Note: If the HSM9E touchscreen is off, tap it once to activate the display. g) When "Register your Partition Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. h) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. k) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. n) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. o) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. t) When HSM9E returns to its dashboard, remove the last iKey of the domain set. <p>Note 1: The "KE-CL" displayed on the dashboard indicates Key Export and Cloning are enabled.</p> <p>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 92.</p>		

Configure HSM9E (Tier 7) Partition Policies

Step	Activity	Initials	Time
3.10	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Log in as the Partition Officer: <code>role login -name po</code> b) Follow the instructions on the HSM9E touchscreen to perform Partition SO authentication: Note: If the HSM9E touchscreen is off, tap it once to activate the display. c) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. f) When HSM9E returns to its dashboard, remove the last iKey of the SO set. g) Using the LunaCM terminal, allow partition activation with PIN: <code>partition changepolicy -policy 22 -value 1</code> <p>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 92.</p>		

Generate HSM9E (Tier 7) CO Credentials and PIN

Step	Activity	Initials	Time
3.11	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the CO role: <code>role init -name co</code> b) Follow the instructions on the HSM9E touchscreen to generate a 3 of 7 CO credential set: Note: If the HSM9E touchscreen is off, tap it once to activate the display. c) When "Register your Crypto Officer..." is displayed, select "Create new quorum of iKeys", then press continue. d) When "How many iKeys will make up the full Crypto Officer?" is displayed, enter 7, then press the ✓ in the lower right corner. e) When "How many iKeys will be required for authentication?" is displayed, enter 3, then press the ✓ in the lower right corner. f) When "Please insert first iKey" is displayed, insert the first CO iKey, then press continue. g) When "Create a new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. h) When "Re-enter your new PIN for this iKey" is displayed, leave the input blank, then press the ✓ in the lower right corner. i) When "First iKey successfully registered" is displayed, remove the iKey, then press continue. j) Repeat steps f) to i) for the 2nd, 3rd, 4th, 5th, 6th, and 7th CO iKeys. k) When "Registration successful" is displayed, press continue. l) Using the LunaCM terminal, configure a CO PIN: <code>role createchallenge -name co</code> m) When "Enter new challenge secret:" is displayed, type 11223344, then press enter. n) When "Re-enter new challenge secret:" is displayed, type 11223344, then press enter. o) Log out of CO role: <code>role logout</code> <p>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 92.</p>		

Clone Recovery Key Share Holder CO iKeys

Step	Activity	Initials	Time
3.12	<p>CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.</p> <p>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.</p> <p>Using the HSM9E touchscreen, CA executes the following steps: Note: If the HSM9E touchscreen is off, tap it once to activate the display.</p> <ol style="list-style-type: none"> a) Select the Admin tab at the top of the display. b) Insert the 1st source iKey to be cloned, then press "Duplicate this iKey". 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. d) Take the 1st recipient iKey from the credential stand, insert it into the HSM, then press continue. e) When "iKey duplicated" is displayed, press continue, then the 1st recipient iKey becomes the 2nd source iKey, so select "Duplicate this iKey". 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. g) Take the 2nd recipient iKey from the credential stand, insert it into the HSM, then press continue. h) When "iKey duplicated" is displayed, press continue, remove the 2nd recipient iKey, then place it on the credential stand. i) Repeat steps b) to h) for the 2nd, 3rd, 4th, 5th, 6th, and 7th iKeys in the CO credential sets. j) Select the Dashboard tab at the top of the display. <p>1st Source: "RKSH CO SET 1" Recipient: "RKSH CO SET 2" 2nd Source: "RKSH CO SET 2" Recipient: "TCR CO SET 1 Copy 1"</p> <p>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 92.</p>		

Clone Recovery Key Share Holder Domain iKeys

Step	Activity	Initials	Time
3.13	<p>CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.</p> <p>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.</p> <p>Using the HSM9E touchscreen, CA executes the following steps: Note: If the HSM9E touchscreen is off, tap it once to activate the display.</p> <ol style="list-style-type: none"> a) Select the Admin tab at the top of the display. b) Insert the 1st source iKey to be cloned, then press "Duplicate this iKey". 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. d) Take the 1st recipient iKey from the credential stand, insert it into the HSM, then press continue. e) When "iKey duplicated" is displayed, press continue, then the 1st recipient iKey becomes the 2nd source iKey, so select "Duplicate this iKey". 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. g) Take the 2nd recipient iKey from the credential stand, insert it into the HSM, then press continue. h) When "iKey duplicated" is displayed, press continue, remove the 2nd recipient iKey, then place it on the credential stand. i) Repeat steps b) to h) for the 2nd, 3rd, 4th, 5th, 6th, and 7th iKeys in the Domain credential sets. j) Select the Dashboard tab at the top of the display. <p>1st Source: "RKSH Domain SET 1" Recipient: "RKSH Domain SET 2" 2nd Source: "RKSH Domain SET 2" Recipient: "TCR Domain SET 1 Copy 1"</p> <p>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 92.</p>		

Place Recovery Key Share Holders' Credentials into TEBs

Step	Activity	Initials	Time
3.14	<p>The CA calls each of the RKSHs listed below sequentially to the ceremony table to perform the following steps:</p> <ol style="list-style-type: none"> 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. 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. c) CA places the backup TEB inside of the primary TEB in case the primary TEB is compromised in the future. d) CA places the RKSH note inside of the primary TEB, ensuring it's still legible through the bag. e) CA along with IW inspects the designated plastic credential case to ensure it contains the CO and Domain iKeys allocated to the RKSH. f) RKSH inspects the designated credential plastic case to ensure it contains their allocated CO and Domain iKeys. g) CA places the plastic case into its designated new TEB, then seals it. h) CA gives the IW sealing strips for post-ceremony inventory. i) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. j) CA initials the TEB with a ballpoint pen. k) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. l) RKSH inspects the TEB, verifies its contents, then initials it with a ballpoint pen. m) RKSH writes the date and time, signs the credential table of the IW's script, then IW initials the entry. n) RKSH returns to their seat with their TEB. o) Repeat steps for all the remaining RKSHs on the list. <p>RKSH1: Sebastian Castro Luna Credential TEB # BB02638647 Luna Credential Backup TEB # BB02638646</p> <p>RKSH2: Ondřej Surý Luna Credential TEB # BB02639616 Luna Credential Backup TEB # BB02639615</p> <p>RKSH3: Kristian Ørmen Luna Credential TEB # BB02639614 Luna Credential Backup TEB # BB02639613</p> <p>RKSH4: Jiankang Yao Luna Credential TEB # BB02639612 Luna Credential Backup TEB # BB02639611</p> <p>RKSH5: Bevil Wooding Luna Credential TEB # BB02639610 Luna Credential Backup TEB # BB02639609</p> <p>RKSH6: John Curran Luna Credential TEB # BB02639608 Luna Credential Backup TEB # BB02639607</p> <p>RKSH7: Dave Lawrence Luna Credential TEB # BB02639606 Luna Credential Backup TEB # BB02639605</p>		

TCR	TEB #	Printed Name	Signature	Date	Time	IW Initials
RKSH1	TEB # BB02638647	Sebastian Castro		2024 Apr __		
RKSH2	TEB # BB02639616	Ondřej Surý		2024 Apr __		
RKSH3	TEB # BB02639614	Kristian Ørmen		2024 Apr __		
RKSH4	TEB # BB02639612	Jiankang Yao		2024 Apr __		
RKSH5	TEB # BB02639610	Bevil Wooding		2024 Apr __		
RKSH6	TEB # BB02639608	John Curran		2024 Apr __		
RKSH7	TEB # BB02639606	Dave Lawrence		2024 Apr __		

Clone Crypto Officer CO iKeys

Step	Activity	Initials	Time
3.15	<p>CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.</p> <p>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.</p> <p>Using the HSM9E touchscreen, CA executes the following steps:</p> <p>Note: If the HSM9E touchscreen is off, tap it once to activate the display.</p> <ol style="list-style-type: none"> a) Select the Admin tab at the top of the display. b) Insert the 1st source iKey to be cloned, then press "Duplicate this iKey". 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. d) Take the 1st recipient iKey from the credential stand, insert it into the HSM, then press continue. e) When "iKey duplicated" is displayed, press continue, then the 1st recipient iKey becomes the 2nd source iKey, so select "Duplicate this iKey". 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. g) Take the 2nd recipient iKey from the credential stand, insert it into the HSM, then press continue. h) When "iKey duplicated" is displayed, press continue, then the 2nd recipient iKey becomes the 3rd source iKey, so select "Duplicate this iKey". 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. j) Insert the 3rd recipient iKey into the HSM, then press continue. k) When "iKey duplicated" is displayed, press continue, remove the 3rd recipient iKey, and place it on the credential stand. l) Repeat steps b) to h) for the 2nd, 3rd, 4th, 5th, 6th, and 7th iKeys in the CO credential sets. m) Select the Dashboard tab at the top of the display. <p>1st Source: "TCR CO SET 1 Copy 1" Recipient: "TCR CO SET 2 Copy 1" 2nd Source: "TCR CO SET 2 Copy 1" Recipient: "TCR CO SET 1 Copy 2" 3rd Source: "TCR CO SET 1 Copy 2" Recipient: "TCR CO SET 2 Copy 2"</p> <p>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 92.</p>		

Clone Crypto Officer SO iKeys

Step	Activity	Initials	Time
3.16	<p>CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.</p> <p>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.</p> <p>Using the HSM9E touchscreen, CA executes the following steps: Note: If the HSM9E touchscreen is off, tap it once to activate the display.</p> <ol style="list-style-type: none"> a) Select the Admin tab at the top of the display. b) Insert the 1st source iKey to be cloned, then press "Duplicate this iKey". 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. d) Take the 1st recipient iKey from the credential stand, insert it into the HSM, then press continue. e) When "iKey duplicated" is displayed, press continue, then the 1st recipient iKey becomes the 2nd source iKey, so select "Duplicate this iKey". 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. g) Take the 2nd recipient iKey from the credential stand, insert it into the HSM, then press continue. h) When "iKey duplicated" is displayed, press continue, then the 2nd recipient iKey becomes the 3rd source iKey, so select "Duplicate this iKey". 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. j) Insert the 3rd recipient iKey into the HSM, then press continue. k) When "iKey duplicated" is displayed, press continue, remove the 3rd recipient iKey, and place it on the credential stand. l) Repeat steps b) to h) for the 2nd, 3rd, 4th, 5th, 6th, and 7th iKeys in the SO credential sets. m) Select the Dashboard tab at the top of the display. <p>1st Source: "TCR SO SET 1 Copy 1" Recipient: "TCR SO SET 2 Copy 1" 2nd Source: "TCR SO SET 2 Copy 1" Recipient: "TCR SO SET 1 Copy 2" 3rd Source: "TCR SO SET 1 Copy 2" Recipient: "TCR SO SET 2 Copy 2"</p> <p>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 92.</p>		

Clone Crypto Officer Audit iKeys

Step	Activity	Initials	Time
3.17	<p>CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.</p> <p>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.</p> <p>Using the HSM9E touchscreen, CA executes the following steps: Note: If the HSM9E touchscreen is off, tap it once to activate the display.</p> <ol style="list-style-type: none"> a) Select the Admin tab at the top of the display. b) Insert the 1st source iKey to be cloned, then press "Duplicate this iKey". 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. d) Take the 1st recipient iKey from the credential stand, insert it into the HSM, then press continue. e) When "iKey duplicated" is displayed, press continue, then the 1st recipient iKey becomes the 2nd source iKey, so select "Duplicate this iKey". 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. g) Take the 2nd recipient iKey from the credential stand, insert it into the HSM, then press continue. h) When "iKey duplicated" is displayed, press continue, then the 2nd recipient iKey becomes the 3rd source iKey, so select "Duplicate this iKey". 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. j) Insert the 3rd recipient iKey into the HSM, then press continue. k) When "iKey duplicated" is displayed, press continue, remove the 3rd recipient iKey, and place it on the credential stand. l) Repeat steps b) to h) for the 2nd, 3rd, 4th, 5th, 6th, and 7th iKeys in the Audit credential sets. m) Select the Dashboard tab at the top of the display. <p>1st Source: "TCR Audit SET 1 Copy 1" Recipient: "TCR Audit SET 2 Copy 1" 2nd Source: "TCR Audit SET 2 Copy 1" Recipient: "TCR Audit SET 1 Copy 2" 3rd Source: "TCR Audit SET 1 Copy 2" Recipient: "TCR Audit SET 2 Copy 2"</p> <p>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 92.</p>		

Clone Crypto Officer Domain iKeys

Step	Activity	Initials	Time
3.18	<p>CA clones the credential sets listed below as specified in sequential order, beginning with the 1st and ending with the 7th iKeys.</p> <p>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.</p> <p>Using the HSM9E touchscreen, CA executes the following steps: Note: If the HSM9E touchscreen is off, tap it once to activate the display.</p> <ol style="list-style-type: none"> a) Select the Admin tab at the top of the display. b) Insert the 1st source iKey to be cloned, then press "Duplicate this iKey". 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. d) Take the 1st recipient iKey from the credential stand, insert it into the HSM, then press continue. e) When "iKey duplicated" is displayed, press continue, then the 1st recipient iKey becomes the 2nd source iKey, so select "Duplicate this iKey". 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. g) Take the 2nd recipient iKey from the credential stand, insert it into the HSM, then press continue. h) When "iKey duplicated" is displayed, press continue, then the 2nd recipient iKey becomes the 3rd source iKey, so select "Duplicate this iKey". 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. j) Insert the 3rd recipient iKey into the HSM, then press continue. k) When "iKey duplicated" is displayed, press continue, remove the 3rd recipient iKey, and place it on the credential stand. l) Repeat steps b) to h) for the 2nd, 3rd, 4th, 5th, 6th, and 7th iKeys in the Domain credential sets. m) Select the Dashboard tab at the top of the display. <p>1st Source: "TCR Domain SET 1 Copy 1" Recipient: "TCR Domain SET 2 Copy 1" 2nd Source: "TCR Domain SET 2 Copy 1" Recipient: "TCR Domain SET 1 Copy 2" 3rd Source: "TCR Domain SET 1 Copy 2" Recipient: "TCR Domain SET 2 Copy 2"</p> <p>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 92.</p>		

Place KMF West Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
3.19	<p>The CA prepares the KMF West Crypto Officer credentials by performing the following steps for each entry listed below:</p> <ul style="list-style-type: none"> 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. b) CA along with IW inspects the designated plastic credential case to ensure it contains the iKeys allocated to the KMF West Crypto Officer. c) CA places the plastic case into its designated new TEB, then seals it. d) CA gives the IW sealing strips for post-ceremony inventory. e) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. f) CA initials the TEB with a ballpoint pen. g) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. h) CA gives the TEB to IW to set aside pending the next step. <p>CO1: Arbogast Fabian TEB # BB02639636</p> <p>CO2: Ralf Weber TEB # BB02639635</p> <p>CO3: João Damas TEB # BB02639634</p> <p>CO4: Carlos Martinez TEB # BB02639633</p> <p>CO5: Ólafur Guðmundsson TEB # BB02639632</p> <p>CO6: Jorge Etges TEB # BB02639631</p> <p>CO7: Subramanian Moonesamy TEB # BB02639630</p>		

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

Step	Activity	Initials	Time
3.20	<p>The CA perform the following steps to place the KMF West Crypto Officer Credentials into overwrap TEBs for transport:</p> <ul style="list-style-type: none"> 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. 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. c) CA gives the IW sealing strips for post-ceremony inventory. d) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. e) CA initials the TEB with a ballpoint pen. f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. g) RKOS initials the TEB, then IW takes custody of the Credential Overwrap TEB #1 for transit to KMF West. 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. 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. j) CA gives the IW sealing strips for post-ceremony inventory. k) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. l) CA initials the TEB with a ballpoint pen. m) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. n) RKOS initials the TEB, then RKOS takes custody of the Credential Overwrap TEB #2 for transit to KMF West. <p>Credential Overwrap #1 TEB # BB02639629 Credential Overwrap #2 TEB # BB02639628</p>		

Lunch Break

Step	Activity	Initials	Time
3.21	<p>CA and IW ensure all ceremony participants are escorted out of Tier 4 (Ceremony Room). Target break window is 30 minutes.</p> <ul style="list-style-type: none"> a) Audit Cameras are never obstructed. b) Live stream audio is muted until the ceremony resumes. <p>RKOS will escort each group of participants out of the ceremony room for the ceremony break.</p>		
3.22	<p>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.</p>		

KSK Generation

Step	Activity	Initials	Time
3.23	<p>Using the LunaCM terminal, CA executes the following steps to generate a new KSK:</p> <ul style="list-style-type: none"> a) Log in with the Crypto Officer role: <code>role login -name co</code> b) When "enter password" is displayed, enter the secret password: <code>11223344</code> c) Follow the instructions on the HSM9E touchscreen to perform CO authentication: Note: If the HSM9E touchscreen is off, tap it once to activate the display. d) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. g) When HSM9E returns to its dashboard, remove the last iKey of the CO set. h) Exit the LunaCM terminal window by typing the following command: <code>exit</code> i) Using the Commands terminal window, execute the command below to change the working directory: <code>cd /media/HSMFD/KSK53-2</code> j) Initiate key generation with the following multi-line command: <code>kskm-keymaster --hsm luna keygen --algorithm RSASHA256 --size 2048</code> k) Verify the presence of the keypair created previously: <code>kskm-keymaster --hsm luna inventory</code> <p>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 92.</p>		

KSK Key Tag Verification

Step	Activity	Initials	Time																
3.24	<p>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:</p> <table border="1"> <thead> <tr> <th>KSK</th> <th>Label</th> <th>Key Tag</th> <th>Revoke</th> </tr> </thead> <tbody> <tr> <td>2010</td> <td>Kjqmt7v</td> <td>19036</td> <td>19164</td> </tr> <tr> <td>2017</td> <td>Klajeyz</td> <td>20326</td> <td>20454</td> </tr> <tr> <td>2023</td> <td>Kmrf13b</td> <td>46211</td> <td>46339</td> </tr> </tbody> </table>	KSK	Label	Key Tag	Revoke	2010	Kjqmt7v	19036	19164	2017	Klajeyz	20326	20454	2023	Kmrf13b	46211	46339		
KSK	Label	Key Tag	Revoke																
2010	Kjqmt7v	19036	19164																
2017	Klajeyz	20326	20454																
2023	Kmrf13b	46211	46339																

Print Copies of the KSK Generation Log

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

Record Key Label

Step	Activity	Initials	Time
3.27	IW records the key label: Root KSK 2024 Label: _____		

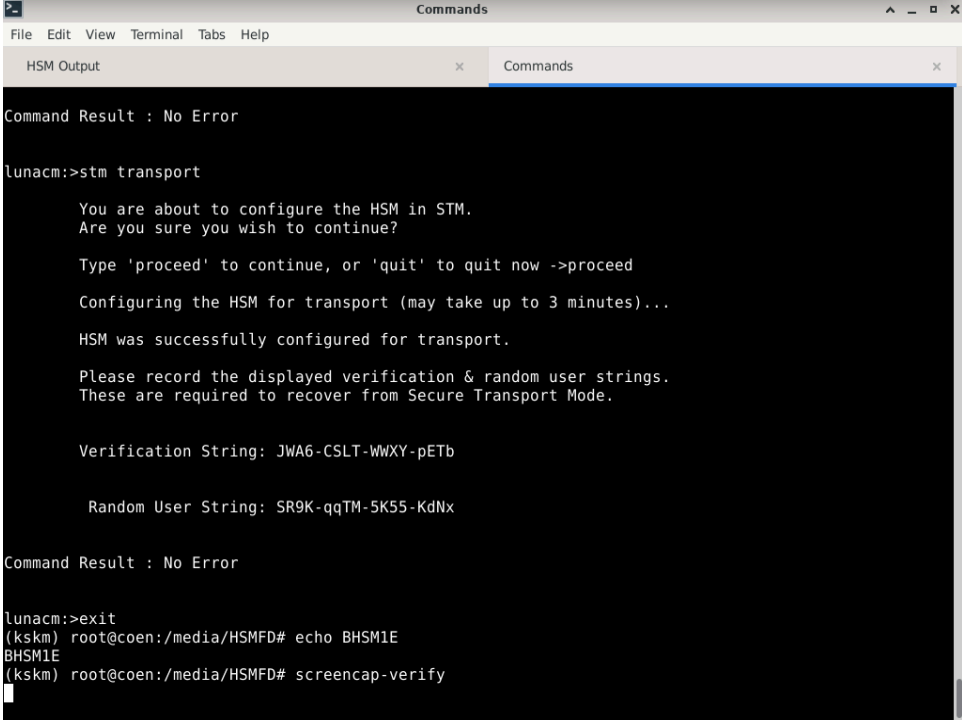
BHSM1E (Tier 7) Setup

Step	Activity	Initials	Time
3.28	<p>CA performs the following steps to prepare BHSM1E:</p> <ul style="list-style-type: none"> a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. 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. e) Read aloud the BHSM1E serial number while IW verifies the information using the previous ceremony script where it was last used. f) Flip BHSM1E over face up in its designated stand. <p>BHSM1E: TEB # BB02638476 / Serial # 706530 Last Verified: AT Ceremony 53-2 2024-03-27</p>		

Power ON BHSM1E (Tier 7)

Step	Activity	Initials	Time
3.29	<p>CA performs the following steps to prepare BHSM1E:</p> <ul style="list-style-type: none"> a) Plug a USB HSM cable into the USB-C port on the top of BHSM1E. b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. c) Wait for BHSM1E to boot and confirm the device is in Secure Transport Mode (STM). d) Verify the displayed HSM serial number on the screen matches 706530. <p>BHSM1E: Serial # 706530</p>		

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

Step	Activity	Initials	Time
<p>3.30</p>	<p>Using the Commands terminal window, CA executes the following steps to recover the HSM from STM:</p> <ol style="list-style-type: none"> Launch the LunaCM application: <code>lunacm</code> Select the BHSM1E: Serial # 706530 admin partition slot: <code>slot set -s 105</code> 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.  <p>Screenshot of BHSM1E STM placement during AT Ceremony 53-2 2024-03-27</p> <ol style="list-style-type: none"> 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 Recover BHSM1E from STM: <code>stm recover -randomuserstring SR9K-qqTM-5K55-KdNx</code> Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step. 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 Once the string is verified type <code>proceed</code>, then press enter to recover BHSM1E from STM. 		

Register BHSM1E (Tier 7) Audit Credentials

Step	Activity	Initials	Time
3.31	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Initialize the audit role: <code>role init -name au</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM1E touchscreen to register a 3 of 7 audit credential set: Note: If the BHSM1E touchscreen is off, tap it once to activate the display. d) When "Register your Auditor..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert audit iKey 1 of 7, then press continue. f) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert audit iKey 2 of 7, then press continue. g) When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert audit iKey 3 of 7, then press continue. h) When BHSM1E returns to its dashboard, remove the last iKey of the audit set. <p>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 92.</p>		

Configure BHSM1E (Tier 7) Audit Settings

Step	Activity	Initials	Time
3.32	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> Log in with the audit role: <code>role login -name au</code> Follow the instructions on the BHSM1E touchscreen to perform audit authentication: Note: If the BHSM1E touchscreen is off, tap it once to activate the display. When "Please ensure an iKey is inserted" is displayed, insert audit iKey 4 of 7, then press continue. When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert audit iKey 5 of 7, then press continue. When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert audit iKey 6 of 7, then press continue. When BHSM1E returns to its dashboard, remove the last iKey of the audit set. Using the LunaCM terminal, synchronize the HSM's clock with the host time: <code>audit time sync</code> Set the filepath where log files are written: <code>audit config path /media/HSMFD/BHSM1E</code> Set audit logging configuration: <code>audit config evmask all,failure,success</code> Type <code>proceed</code>, then press enter to continue. Set audit logging rotation interval: <code>audit config interval hourly@00</code> Set audit logging maximum log file size: <code>audit config size 4096k</code> Show the audit logging configuration: <code>audit config get</code> Confirm with IW the output of the logging configuration matches with the list below: <pre> 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 </pre> <p>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 92.</p>		

Initialize BHSM1E (Tier 7) Administrative Partition

Step	Activity	Initials	Time
3.33	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the BHSM1E administrative partition: <code>hsm init -label BHSM1E -iped</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM1E touchscreen to register a 3 of 7 SO and 5 of 7 domain credential set: Note: If the BHSM1E touchscreen is off, tap it once to activate the display. d) When "Register your Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert SO iKey 1 of 7, then press continue. f) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert SO iKey 2 of 7, then press continue. 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. h) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. i) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey, insert SO iKey 4 of 7, then press continue. 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. k) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. l) When "Please insert first iKey" is displayed, insert domain iKey 1 of 7, then press continue. m) When "Please insert iKey 2 of 5" is displayed, remove the previous iKey and insert domain iKey 2 of 7, then press continue. n) When "Please insert iKey 3 of 5" is displayed, remove the previous iKey and insert domain iKey 3 of 7, then press continue. o) When "Please insert iKey 4 of 5" is displayed, remove the previous iKey and insert domain iKey 4 of 7, then press continue. p) When "Please insert iKey 5 of 5" is displayed, remove the previous iKey and insert domain iKey 5 of 7, then press continue. q) When BHSM1E returns to its dashboard, remove the last iKey of the domain set. <p>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 92.</p>		

Configure BHSM1E (Tier 7) Global Policies

Step	Activity	Initials	Time
3.34	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the BHSM1E admin partition slot number: <code>slot list</code> b) Select the BHSM1E admin partition slot: <code>slot set -s 105</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the BHSM1E touchscreen to perform SO authentication: Note: If the BHSM1E touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert SO iKey 6 of 7, then press continue. f) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert SO iKey 7 of 7, then press continue. 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. h) When BHSM1E returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, activate FIPS mode: <code>hsm changehsmpolicy -policy 55 -value 1</code> j) Verify BHSM1E is in FIPS approved operation mode: <code>hsm showinfo</code> <p>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 92.</p>		

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

Step	Activity	Initials	Time
3.35	<p>Using the LunaCM terminal, CA executes the following steps to perform CO authentication:</p> <ul style="list-style-type: none"> a) Verify the application partition slot number: <code>slot list</code> b) Select the HSM's application partition slot: <code>slot set -s 3</code> c) Log in with the Crypto Officer role: <code>role login -name co</code> d) When "enter password" is displayed, enter the secret password: <code>11223344</code> e) Show the KSK key pair: <code>partition contents</code> f) Match the displayed KSK label with the key label indicated on step 3.27 		

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

Step	Activity	Initials	Time
3.36	<p>Using the LunaCM terminal, CA executes the following steps to back up KSK key pair:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initiate the backup from the HSM application partition to BHSM1E: <code>partition archive backup -slot 105 -partition KSK-2024</code> b) Follow the instructions on the BHSM1E touchscreen to register and authenticate SO, Partition SO, domain, and CO credential sets: Note: If the BHSM1E touchscreen is off, tap it once to activate the display. c) When "Please ensure an iKey is inserted" is displayed, begin SO registration by inserting a randomly selected SO iKey, then press continue. 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. 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. f) When "Register your Partition Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. g) When "Please insert first iKey" is displayed, leave the current iKey inserted, then press continue. 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. 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. j) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. <p style="text-align: right;"><i>Continued on next page</i></p>		

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

Step	Activity	Initials	Time
3.37	<ul style="list-style-type: none"> a) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. b) When "Please insert first iKey" is displayed, insert domain iKey 6 of 7, then press continue. c) When "Please insert iKey 2 of 5" is displayed, remove the previous iKey and insert domain iKey 7 of 7, then press continue. 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. 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. 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. g) When "Please ensure an iKey is inserted" is displayed, remove the previous iKey and insert a randomly selected SO iKey, then press continue. 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. 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. 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. k) When "Please insert first iKey" is displayed, insert CO iKey 1 of 7, then press continue. l) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert CO iKey 2 of 7, then press continue. 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. n) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. o) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert CO iKey 4 of 7, then press continue. p) When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert CO iKey 5 of 7, then press continue. q) When BHSM1E returns to its dashboard, remove the last iKey of the CO set. 		

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

Step	Activity	Initials	Time
3.38	<p>Using the LunaCM terminal, CA executes the following steps to verify the KSK key pair:</p> <ul style="list-style-type: none"> a) List the backups in BHSM1E by specifying BHSM1E's slot number: <code>partition archive list -slot 105</code> b) List the contents of the backups in BHSM1E: <code>partition archive contents -slot 105 -partition KSK-2024</code> c) Follow the instructions on the BHSM1E touchscreen to perform CO authentication: Note: If the BHSM1E touchscreen is off, tap it once to activate the display. d) When "Please ensure an iKey is inserted" is displayed, insert CO iKey 6 of 7, then press continue. e) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert CO iKey 7 of 7, then press continue. 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. g) When BHSM1E returns to its dashboard, remove the last iKey of the CO set. h) Match the displayed KSK label with the key label indicated on step 3.27 		

Place BHSM1E (Tier 7) in the TEB

Step	Activity	Initials	Time
3.39	<p>CA performs the following steps to prepare BHSM1E for storage:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: <code>exit</code> b) Unplug the HSM cable from the upper USB-C port of BHSM1E. 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. d) Read aloud the HSM serial number while the IW verifies it matches the information below. e) Place the HSM into its designated new TEB, then seal it. f) Give IW the sealing strips for post-ceremony inventory. g) Place the HSM onto its designated space on the ceremony table visible to the audit camera. h) Initial the TEB along with IW using a ballpoint pen. i) Place the HSM TEB on the cart. <p>BHSM1E: TEB # BB02639622 / Serial # 706530</p>		

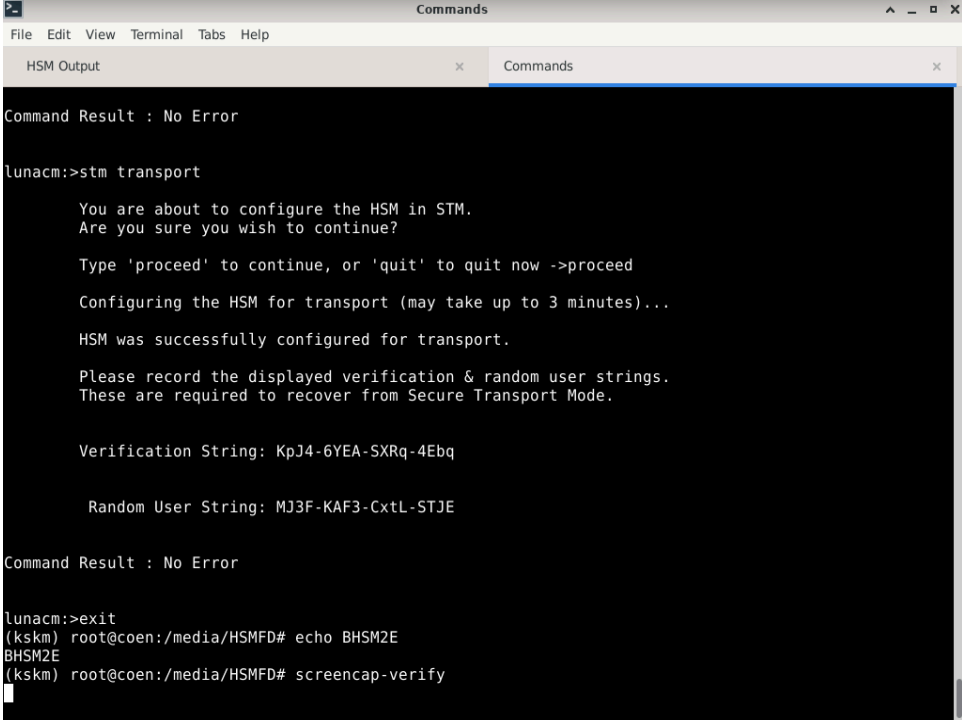
BHSM2E (Tier 7) Setup

Step	Activity	Initials	Time
3.40	<p>CA performs the following steps to prepare BHSM2E:</p> <ul style="list-style-type: none"> a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. 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. e) Read aloud the BHSM2E serial number while IW verifies the information using the previous ceremony script where it was last used. f) Flip BHSM2E over face up in its designated stand. <p>BHSM2E: TEB # BB02638475 / Serial # 718029 Last Verified: AT Ceremony 53-2 2024-03-27</p>		

Power ON BHSM2E (Tier 7)

Step	Activity	Initials	Time
3.41	<p>CA performs the following steps to prepare BHSM2E:</p> <ul style="list-style-type: none"> a) Plug a USB HSM cable into the USB-C port on the top of BHSM2E. b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. c) Wait for BHSM2E to boot and confirm the device is in Secure Transport Mode (STM). d) Verify the displayed HSM serial number on the screen matches 718029. <p>BHSM2E: Serial # 718029</p>		

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

Step	Activity	Initials	Time
<p>3.42</p>	<p>Using the Commands terminal window, CA executes the following steps to recover the HSM from STM:</p> <ol style="list-style-type: none"> Launch the LunaCM application: <code>lunacm</code> Select the BHSM2E: Serial # 718029 admin partition slot: <code>slot set -s 105</code> 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.  <p>Screenshot of BHSM2E STM placement during AT Ceremony 53-2 2024-03-27</p> <ol style="list-style-type: none"> 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 Recover BHSM2E from STM: <code>stm recover -randomuserstring MJ3F-KAF3-CxtL-STJE</code> Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step. 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 Once the string is verified type <code>proceed</code>, then press enter to recover BHSM2E from STM. 		

Register BHSM2E (Tier 7) Audit Credentials

Step	Activity	Initials	Time
3.43	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Initialize the audit role: <code>role init -name au</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM2E touchscreen to register a 3 of 7 audit credential set: Note: If the BHSM2E touchscreen is off, tap it once to activate the display. d) When "Register your Auditor..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert audit iKey 7 of 7, then press continue. 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. 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. h) When BHSM2E returns to its dashboard, remove the last iKey of the audit set. <p>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 92.</p>		

Configure BHSM2E (Tier 7) Audit Settings

Step	Activity	Initials	Time
3.44	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> Log in with the audit role: <code>role login -name au</code> Follow the instructions on the BHSM2E touchscreen to perform audit authentication: Note: If the BHSM2E touchscreen is off, tap it once to activate the display. When "Please ensure an iKey is inserted" is displayed, insert a randomly selected audit iKey, then press continue. When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When BHSM2E returns to its dashboard, remove the last iKey of the audit set. Using the LunaCM terminal, synchronize the HSM's clock with the host time: <code>audit time sync</code> Set the filepath where log files are written: <code>audit config path /media/HSMFD/BHSM2E</code> Set audit logging configuration: <code>audit config evmask all,failure,success</code> Type <code>proceed</code>, then press enter to continue. Set audit logging rotation interval: <code>audit config interval hourly@00</code> Set audit logging maximum log file size: <code>audit config size 4096k</code> Show the audit logging configuration: <code>audit config get</code> Confirm with IW the output of the logging configuration matches with the list below: <pre> 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 </pre> <p>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 92.</p>		

Initialize BHSM2E (Tier 7) Administrative Partition

Step	Activity	Initials	Time
3.45	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the BHSM2E administrative partition: <code>hsm init -label BHSM2E -iped</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM2E touchscreen to register a 3 of 7 SO and 5 of 7 domain credential set: Note: If the BHSM2E touchscreen is off, tap it once to activate the display. d) When "Register your Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. i) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey, insert a different randomly selected SO iKey, then press continue. 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. k) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. l) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. q) When BHSM2E returns to its dashboard, remove the last iKey of the domain set. <p>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 92.</p>		

Configure BHSM2E (Tier 7) Global Policies

Step	Activity	Initials	Time
3.46	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the BHSM2E admin partition slot number: <code>slot list</code> b) Select the BHSM2E admin partition slot: <code>slot set -s 105</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the BHSM2E touchscreen to perform SO authentication: Note: If the BHSM2E touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When BHSM2E returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, activate FIPS mode: <code>hsm changehsmpolicy -policy 55 -value 1</code> j) Verify BHSM2E is in FIPS approved operation mode: <code>hsm showinfo</code> <p>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 92.</p>		

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

Step	Activity	Initials	Time
3.47	<p>Using the LunaCM terminal, CA executes the following steps to perform CO authentication:</p> <ul style="list-style-type: none"> a) Verify the application partition slot number: <code>slot list</code> b) Select the HSM's application partition slot: <code>slot set -s 3</code> c) Log in with the Crypto Officer role: <code>role login -name co</code> d) When "enter password" is displayed, enter the secret password: <code>11223344</code> e) Show the KSK key pair: <code>partition contents</code> f) Match the displayed KSK label with the key label indicated on step 3.27 		

Back Up KSK Key Pair to BHS2E (Tier 7) 2/3

Step	Activity	Initials	Time
3.48	<p>Using the LunaCM terminal, CA executes the following steps to back up KSK key pair:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initiate the backup from the HSM application partition to BHS2E: <code>partition archive backup -slot 105 -partition KSK-2024</code> b) Follow the instructions on the BHS2E touchscreen to register and authenticate SO, Partition SO, domain, and CO credential sets: Note: If the BHS2E touchscreen is off, tap it once to activate the display. c) When "Please ensure an iKey is inserted" is displayed, begin SO registration by inserting a randomly selected SO iKey, then press continue. 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. 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. f) When "Register your Partition Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. g) When "Please insert first iKey" is displayed, leave the current iKey inserted, then press continue. 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. 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. j) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. <p style="text-align: right;"><i>Continued on next page</i></p>		

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

Step	Activity	Initials	Time
3.49	<ul style="list-style-type: none"> a) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. b) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. g) When "Please ensure an iKey is inserted" is displayed, remove the previous iKey and insert a randomly selected SO iKey, then press continue. 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. 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. 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. k) When "Please insert first iKey" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. n) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. q) When BHSM2E returns to its dashboard, remove the last iKey of the CO set. 		

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

Step	Activity	Initials	Time
3.50	<p>Using the LunaCM terminal, CA executes the following steps to verify the KSK key pair:</p> <ul style="list-style-type: none"> a) List the backups in BHSM2E by specifying BHSM2E's slot number: <code>partition archive list -slot 105</code> b) List the contents of the backups in BHSM2E: <code>partition archive contents -slot 105 -partition KSK-2024</code> c) Follow the instructions on the BHSM2E touchscreen to perform CO authentication: Note: If the BHSM2E touchscreen is off, tap it once to activate the display. d) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. g) When BHSM2E returns to its dashboard, remove the last iKey of the CO set. h) Match the displayed KSK label with the key label indicated on step 3.27 		

Place BHSM2E (Tier 7) in the TEB

Step	Activity	Initials	Time
3.51	<p>CA performs the following steps to prepare BHSM2E for storage:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: <code>exit</code> b) Unplug the HSM cable from the upper USB-C port of BHSM2E. 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. d) Read aloud the HSM serial number while the IW verifies it matches the information below. e) Place the HSM into its designated new TEB, then seal it. f) Give IW the sealing strips for post-ceremony inventory. g) Place the HSM onto its designated space on the ceremony table visible to the audit camera. h) Initial the TEB along with IW using a ballpoint pen. i) Place the HSM TEB on the cart. <p>BHSM2E: TEB # BB02639621 / Serial # 718029</p>		

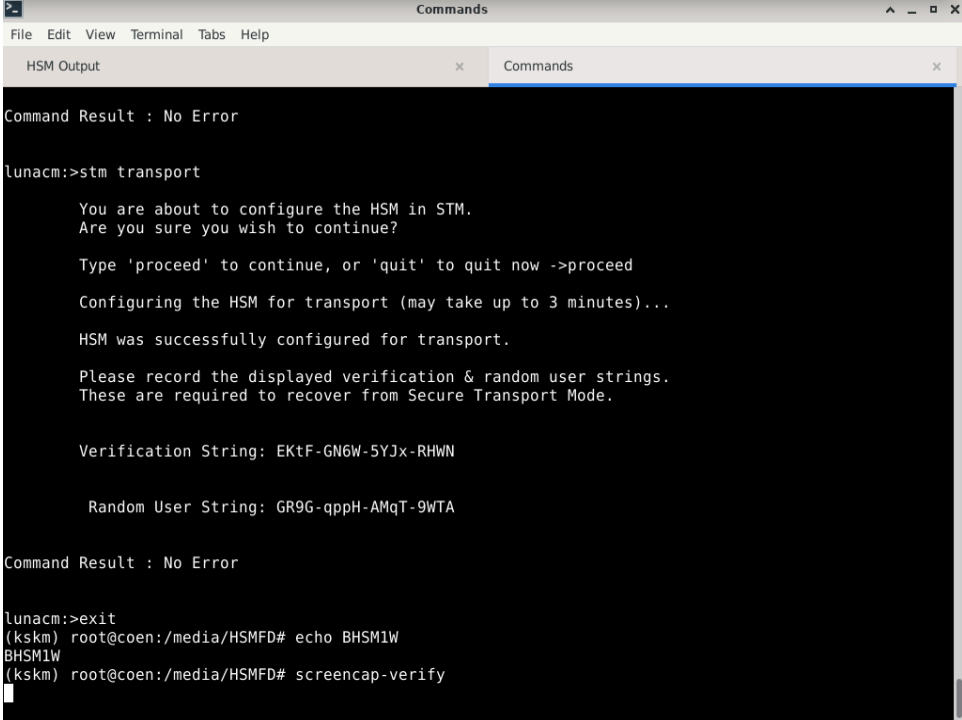
BHSM1W (Tier 7) Setup

Step	Activity	Initials	Time
3.52	<p>CA performs the following steps to prepare BHSM1W:</p> <ul style="list-style-type: none"> a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. 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. e) Read aloud the BHSM1W serial number while IW verifies the information using the previous ceremony script where it was last used. f) Flip BHSM1W over face up in its designated stand. <p>BHSM1W: TEB # BB02638474 / Serial # 718041 Last Verified: AT Ceremony 53-2 2024-03-27</p>		

Power ON BHSM1W (Tier 7)

Step	Activity	Initials	Time
3.53	<p>CA performs the following steps to prepare BHSM1W:</p> <ul style="list-style-type: none"> a) Plug a USB HSM cable into the USB-C port on the top of BHSM1W. b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. c) Wait for BHSM1W to boot and confirm the device is in Secure Transport Mode (STM). d) Verify the displayed HSM serial number on the screen matches 718041. <p>BHSM1W: Serial # 718041</p>		

Recover BHS1W (Tier 7) from Secure Transport Mode (STM)

Step	Activity	Initials	Time
<p>3.54</p>	<p>Using the Commands terminal window, CA executes the following steps to recover the HSM from STM:</p> <ol style="list-style-type: none"> Launch the LunaCM application: <code>lunacm</code> Select the BHS1W: Serial # 718041 admin partition slot: <code>slot set -s 105</code> 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.  <p>Screenshot of BHS1W STM placement during AT Ceremony 53-2 2024-03-27</p> <ol style="list-style-type: none"> 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 Recover BHS1W from STM: <code>stm recover -randomuserstring GR9G-qppH-AMqT-9WTA</code> Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step. 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 Once the string is verified type <code>proceed</code>, then press enter to recover BHS1W from STM. 		

Register BHSM1W (Tier 7) Audit Credentials

Step	Activity	Initials	Time
3.55	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Initialize the audit role: <code>role init -name au</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM1W touchscreen to register a 3 of 7 audit credential set: Note: If the BHSM1W touchscreen is off, tap it once to activate the display. d) When "Register your Auditor..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected audit iKey, then press continue. 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. 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. h) When BHSM1W returns to its dashboard, remove the last iKey of the audit set. <p>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 92.</p>		

Configure BHS1W (Tier 7) Audit Settings

Step	Activity	Initials	Time
3.56	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> Log in with the audit role: <code>role login -name au</code> Follow the instructions on the BHS1W touchscreen to perform audit authentication: Note: If the BHS1W touchscreen is off, tap it once to activate the display. When "Please ensure an iKey is inserted" is displayed, insert a randomly selected audit iKey, then press continue. When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When BHS1W returns to its dashboard, remove the last iKey of the audit set. Using the LunaCM terminal, synchronize the HSM's clock with the host time: <code>audit time sync</code> Set the filepath where log files are written: <code>audit config path /media/HSMFD/BHS1W</code> Set audit logging configuration: <code>audit config evmask all,failure,success</code> Type <code>proceed</code>, then press enter to continue. Set audit logging rotation interval: <code>audit config interval hourly@00</code> Set audit logging maximum log file size: <code>audit config size 4096k</code> Show the audit logging configuration: <code>audit config get</code> Confirm with IW the output of the logging configuration matches with the list below: <pre> Current Logging Configuration ----- event mask : Log everything rotation interval : hourly@ 0 minutes past the hour rotation size (MB) : 4 path to log : /media/HSMFD/BHS1W Command Result : No Error </pre> <p>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 92.</p>		

Initialize BHSM1W (Tier 7) Administrative Partition

Step	Activity	Initials	Time
3.57	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the BHSM1W administrative partition: <code>hsm init -label BHSM1W -iped</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM1W touchscreen to register a 3 of 7 SO and 5 of 7 domain credential set: Note: If the BHSM1W touchscreen is off, tap it once to activate the display. d) When "Register your Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. i) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey, insert a different randomly selected SO iKey, then press continue. 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. k) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. l) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. q) When BHSM1W returns to its dashboard, remove the last iKey of the domain set. <p>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 92.</p>		

Configure BHSM1W (Tier 7) Global Policies

Step	Activity	Initials	Time
3.58	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the BHSM1W admin partition slot number: <code>slot list</code> b) Select the BHSM1W admin partition slot: <code>slot set -s 105</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the BHSM1W touchscreen to perform SO authentication: Note: If the BHSM1W touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When BHSM1W returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, activate FIPS mode: <code>hsm changehsmpolicy -policy 55 -value 1</code> j) Verify BHSM1W is in FIPS approved operation mode: <code>hsm showinfo</code> <p>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 92.</p>		

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

Step	Activity	Initials	Time
3.59	<p>Using the LunaCM terminal, CA executes the following steps to perform CO authentication:</p> <ul style="list-style-type: none"> a) Verify the application partition slot number: <code>slot list</code> b) Select the HSM's application partition slot: <code>slot set -s 3</code> c) Log in with the Crypto Officer role: <code>role login -name co</code> d) When "enter password" is displayed, enter the secret password: <code>11223344</code> e) Show the KSK key pair: <code>partition contents</code> f) Match the displayed KSK label with the key label indicated on step 3.27 		

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

Step	Activity	Initials	Time
3.60	<p>Using the LunaCM terminal, CA executes the following steps to back up KSK key pair:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initiate the backup from the HSM application partition to BHSM1W: <code>partition archive backup -slot 105 -partition KSK-2024</code> b) Follow the instructions on the BHSM1W touchscreen to register and authenticate SO, Partition SO, domain, and CO credential sets: Note: If the BHSM1W touchscreen is off, tap it once to activate the display. c) When "Please ensure an iKey is inserted" is displayed, begin SO registration by inserting a randomly selected SO iKey, then press continue. 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. 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. f) When "Register your Partition Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. g) When "Please insert first iKey" is displayed, leave the current iKey inserted, then press continue. 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. 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. j) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. <p style="text-align: right;"><i>Continued on next page</i></p>		

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

Step	Activity	Initials	Time
3.61	<ul style="list-style-type: none"> a) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. b) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. g) When "Please ensure an iKey is inserted" is displayed, remove the previous iKey and insert a randomly selected SO iKey, then press continue. 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. 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. 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. k) When "Please insert first iKey" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. n) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. q) When BHSM1W returns to its dashboard, remove the last iKey of the CO set. 		

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

Step	Activity	Initials	Time
3.62	<p>Using the LunaCM terminal, CA executes the following steps to verify the KSK key pair:</p> <ul style="list-style-type: none"> a) List the backups in BHSM1W by specifying BHSM1W's slot number: <code>partition archive list -slot 105</code> b) List the contents of the backups in BHSM1W: <code>partition archive contents -slot 105 -partition KSK-2024</code> c) Follow the instructions on the BHSM1W touchscreen to perform CO authentication: Note: If the BHSM1W touchscreen is off, tap it once to activate the display. d) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. g) When BHSM1W returns to its dashboard, remove the last iKey of the CO set. h) Match the displayed KSK label with the key label indicated on step 3.27 		

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

Step	Activity	Initials	Time
3.63	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the admin partition slot number: <code>slot list</code> b) Select the BHSM1W application partition slot: <code>slot set -s 105</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the BHSM1W touchscreen to perform SO authentication: Note: If the BHSM1W touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When BHSM1W returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, place BHSM1W into STM: <code>stm transport</code> j) Type <code>proceed</code>, then press enter to continue. 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. 		

Print BHSM1W Secure Transport Mode (STM) Strings

Step	Activity	Initials	Time
3.64	<p>CA executes the following steps:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: exit b) Using the Commands terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot): echo BHSM1W c) Print two copies of the STM strings, then verify the screenshot: screencap-verify <p>Note: One copy for the audit bundle and one copy for the BHSM1W TEB.</p> <ul style="list-style-type: none"> d) Upon successful verification of the screenshot, close the image viewer application. 		

Place BHSM1W (Tier 7) in the TEB

Step	Activity	Initials	Time
3.65	<p>CA performs the following steps to prepare BHSM1W for storage:</p> <ul style="list-style-type: none"> a) Unplug the HSM cable from the upper USB-C port of BHSM1W. 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. c) Read aloud the HSM serial number while the IW verifies it matches the information below. d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. e) Give IW the sealing strips for post-ceremony inventory. f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. g) Initial the TEB along with IW using a ballpoint pen. h) Call RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. i) Give RKOS the TEB. <p>BHSM1W: TEB # BB02639620 / Serial # 718041</p>		

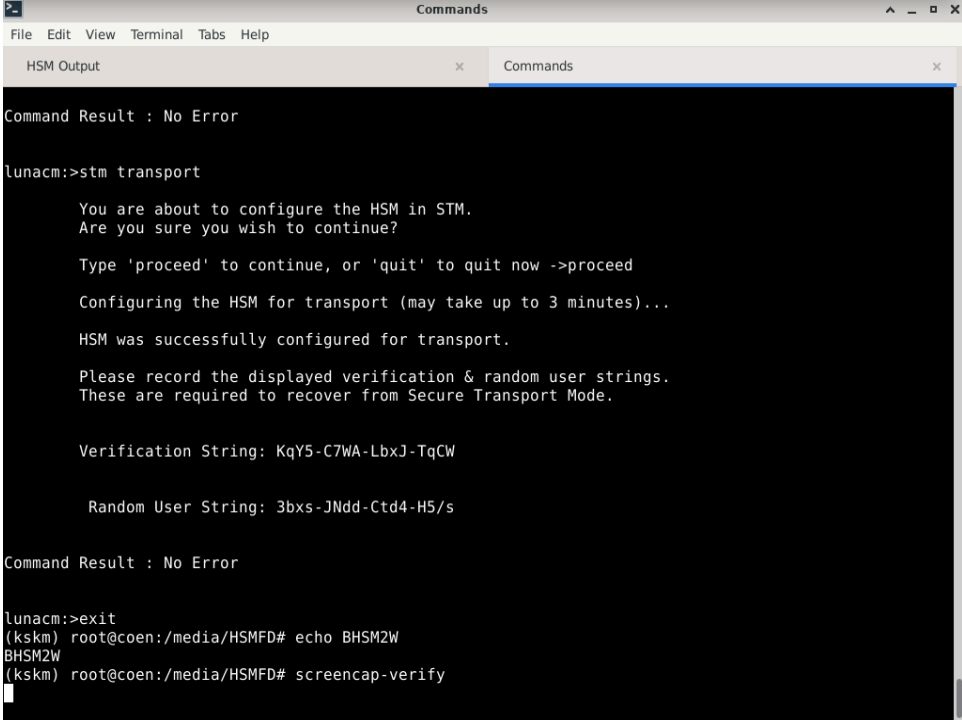
BHSM2W (Tier 7) Setup

Step	Activity	Initials	Time
3.66	<p>CA performs the following steps to prepare BHSM2W:</p> <ul style="list-style-type: none"> a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. 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. e) Read aloud the BHSM2W serial number while IW verifies the information using the previous ceremony script where it was last used. f) Flip BHSM2W over face up in its designated stand. <p>BHSM2W: TEB # BB02638473 / Serial # 718018 Last Verified: AT Ceremony 53-2 2024-03-27</p>		

Power ON BHSM2W (Tier 7)

Step	Activity	Initials	Time
3.67	<p>CA performs the following steps to prepare BHSM2W:</p> <ul style="list-style-type: none"> a) Plug a USB HSM cable into the USB-C port on the top of BHSM2W. b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. c) Wait for BHSM2W to boot and confirm the device is in Secure Transport Mode (STM). d) Verify the displayed HSM serial number on the screen matches 718018. <p>BHSM2W: Serial # 718018</p>		

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

Step	Activity	Initials	Time
<p>3.68</p>	<p>Using the Commands terminal window, CA executes the following steps to recover the HSM from STM:</p> <ol style="list-style-type: none"> Launch the LunaCM application: <code>lunacm</code> Select the BHSM2W: Serial # 718018 admin partition slot: <code>slot set -s 105</code> 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.  <p>Screenshot of BHSM2W STM placement during AT Ceremony 53-2 2024-03-27</p> <ol style="list-style-type: none"> 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. <code>3bxs-JNdd-Ctd4-H5/s</code> Recover BHSM2W from STM: <code>stm recover -randomuserstring 3bxs-JNdd-Ctd4-H5/s</code> Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step. IW confirms that the result matches the Verification string using the printed screenshot from AT Ceremony 53-2 2024-03-27. <code>KqY5-C7WA-LbxJ-TqCW</code> Once the string is verified type <code>proceed</code>, then press enter to recover BHSM2W from STM. 		

Register BHSM2W (Tier 7) Audit Credentials

Step	Activity	Initials	Time
3.69	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Initialize the audit role: <code>role init -name au</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM2W touchscreen to register a 3 of 7 audit credential set: Note: If the BHSM2W touchscreen is off, tap it once to activate the display. d) When "Register your Auditor..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected audit iKey, then press continue. 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. 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. h) When BHSM2W returns to its dashboard, remove the last iKey of the audit set. <p>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 92.</p>		

Configure BHS2W (Tier 7) Audit Settings

Step	Activity	Initials	Time
3.70	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> Log in with the audit role: <code>role login -name au</code> Follow the instructions on the BHS2W touchscreen to perform audit authentication: Note: If the BHS2W touchscreen is off, tap it once to activate the display. When "Please ensure an iKey is inserted" is displayed, insert a randomly selected audit iKey, then press continue. When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When BHS2W returns to its dashboard, remove the last iKey of the audit set. Using the LunaCM terminal, synchronize the HSM's clock with the host time: <code>audit time sync</code> Set the filepath where log files are written: <code>audit config path /media/HSMFD/BHS2W</code> Set audit logging configuration: <code>audit config evmask all,failure,success</code> Type <code>proceed</code>, then press enter to continue. Set audit logging rotation interval: <code>audit config interval hourly@00</code> Set audit logging maximum log file size: <code>audit config size 4096k</code> Show the audit logging configuration: <code>audit config get</code> Confirm with IW the output of the logging configuration matches with the list below: <pre> Current Logging Configuration ----- event mask : Log everything rotation interval : hourly@ 0 minutes past the hour rotation size (MB) : 4 path to log : /media/HSMFD/BHS2W Command Result : No Error </pre> <p>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 92.</p>		

Initialize BHSM2W (Tier 7) Administrative Partition

Step	Activity	Initials	Time
3.71	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the BHSM2W administrative partition: <code>hsm init -label BHSM2W -iped</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the BHSM2W touchscreen to register a 3 of 7 SO and 5 of 7 domain credential set: Note: If the BHSM2W touchscreen is off, tap it once to activate the display. d) When "Register your Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. i) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey, insert a different randomly selected SO iKey, then press continue. 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. k) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. l) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. q) When BHSM2W returns to its dashboard, remove the last iKey of the domain set. <p>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 92.</p>		

Configure BHSM2W (Tier 7) Global Policies

Step	Activity	Initials	Time
3.72	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the BHSM2W admin partition slot number: <code>slot list</code> b) Select the BHSM2W admin partition slot: <code>slot set -s 105</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the BHSM2W touchscreen to perform SO authentication: Note: If the BHSM2W touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When BHSM2W returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, activate FIPS mode: <code>hsm changehsmpolicy -policy 55 -value 1</code> j) Verify BHSM2W is in FIPS approved operation mode: <code>hsm showinfo</code> <p>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 92.</p>		

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

Step	Activity	Initials	Time
3.73	<p>Using the LunaCM terminal, CA executes the following steps to perform CO authentication:</p> <ul style="list-style-type: none"> a) Verify the application partition slot number: <code>slot list</code> b) Select the HSM's application partition slot: <code>slot set -s 3</code> c) Log in with the Crypto Officer role: <code>role login -name co</code> d) When "enter password" is displayed, enter the secret password: <code>11223344</code> e) Show the KSK key pair: <code>partition contents</code> f) Match the displayed KSK label with the key label indicated on step 3.27 		

Back Up KSK Key Pair to BHS2W (Tier 7) 2/3

Step	Activity	Initials	Time
3.74	<p>Using the LunaCM terminal, CA executes the following steps to back up KSK key pair:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initiate the backup from the HSM application partition to BHS2W: <code>partition archive backup -slot 105 -partition KSK-2024</code> b) Follow the instructions on the BHS2W touchscreen to register and authenticate SO, Partition SO, domain, and CO credential sets: Note: If the BHS2W touchscreen is off, tap it once to activate the display. c) When "Please ensure an iKey is inserted" is displayed, begin SO registration by inserting a randomly selected SO iKey, then press continue. 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. 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. f) When "Register your Partition Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. g) When "Please insert first iKey" is displayed, leave the current iKey inserted, then press continue. 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. 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. j) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. <p style="text-align: right;"><i>Continued on next page</i></p>		

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

Step	Activity	Initials	Time
3.75	<ul style="list-style-type: none"> a) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. b) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. g) When "Please ensure an iKey is inserted" is displayed, remove the previous iKey and insert a randomly selected SO iKey, then press continue. 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. 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. 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. k) When "Please insert first iKey" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. n) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. q) When BHSM2W returns to its dashboard, remove the last iKey of the CO set. 		

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

Step	Activity	Initials	Time
3.76	<p>Using the LunaCM terminal, CA executes the following steps to verify the KSK key pair:</p> <ul style="list-style-type: none"> a) List the backups in BHSM2W by specifying BHSM2W's slot number: <code>partition archive list -slot 105</code> b) List the contents of the backups in BHSM2W: <code>partition archive contents -slot 105 -partition KSK-2024</code> c) Follow the instructions on the BHSM2W touchscreen to perform CO authentication: Note: If the BHSM2W touchscreen is off, tap it once to activate the display. d) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. g) When BHSM2W returns to its dashboard, remove the last iKey of the CO set. h) Match the displayed KSK label with the key label indicated on step 3.27 		

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

Step	Activity	Initials	Time
3.77	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the admin partition slot number: <code>slot list</code> b) Select the HSM9E application partition slot: <code>slot set -s 3</code> c) Deactivate the CO role: <code>role deactivate -name co</code> d) Select the HSM9E admin partition slot: <code>slot set -s 4</code> e) Log in with the Security Officer role: <code>role login -name so</code> f) Follow the instructions on the HSM9E touchscreen to perform SO authentication: Note: If the HSM9E touchscreen is off, tap it once to activate the display. g) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. j) When HSM9E returns to its dashboard, remove the last iKey of the SO set. k) Using the LunaCM terminal, place HSM9E into STM: <code>stm transport</code> l) Type <code>proceed</code>, then press enter to continue. 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. 		

Print HSM9E Secure Transport Mode (STM) Strings

Step	Activity	Initials	Time
3.78	<p>CA executes the following steps:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: exit b) Using the Commands terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot): echo HSM9E c) Print two copies of the STM strings, then verify the screenshot: screencap-verify <p>Note: One copy for the audit bundle and one copy for the HSM9E TEB.</p> <ul style="list-style-type: none"> d) Upon successful verification of the screenshot, close the image viewer application. 		

Place HSM9E (Tier 7) in the TEB

Step	Activity	Initials	Time
3.79	<p>CA performs the following steps to prepare HSM9E for storage:</p> <ul style="list-style-type: none"> a) Unplug the HSM cable from the upper USB-C port of HSM9E. 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. c) Read aloud the HSM serial number while the IW verifies it matches the information below. d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. e) Give IW the sealing strips for post-ceremony inventory. f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. g) Initial the TEB along with IW using a ballpoint pen. h) Place the HSM TEB on the cart. <p>HSM9E: TEB # BB02639624 / Serial # 712482</p>		

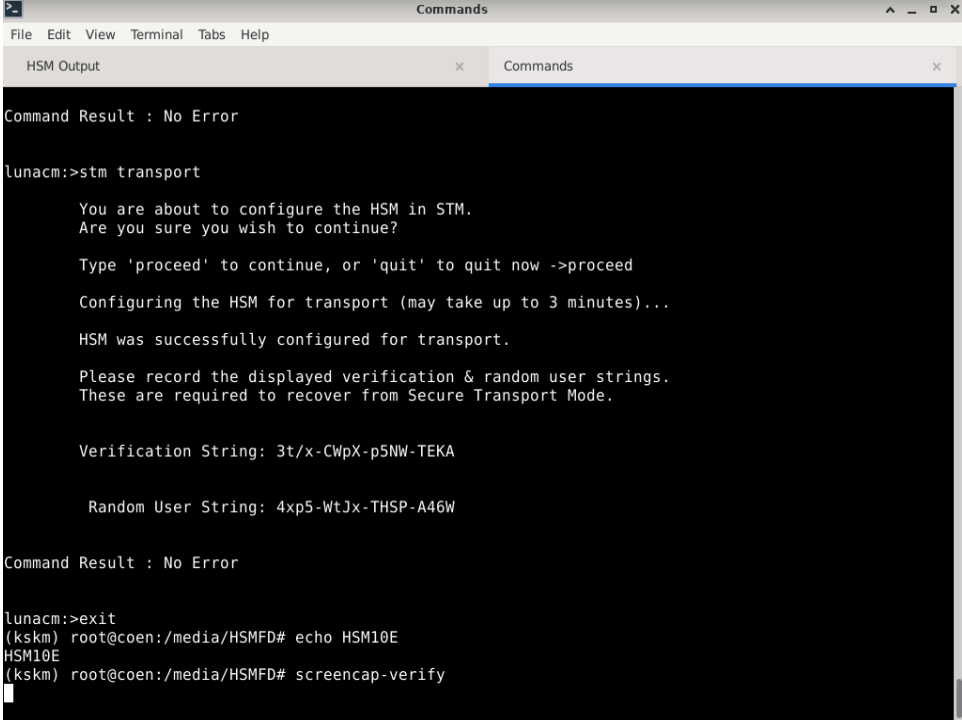
HSM10E (Tier 7) Setup

Step	Activity	Initials	Time
3.80	<p>CA performs the following steps to prepare HSM10E:</p> <ul style="list-style-type: none"> a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. 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. e) Read aloud the HSM10E serial number while IW verifies the information using the previous ceremony script where it was last used. f) Flip HSM10E over face up in its designated stand. <p>HSM10E: TEB # BB02638472 / Serial # 712477 Last Verified: AT Ceremony 53-2 2024-03-27</p>		

Power ON HSM10E (Tier 7)

Step	Activity	Initials	Time
3.81	<p>CA performs the following steps to prepare HSM10E:</p> <ul style="list-style-type: none"> a) Plug a USB HSM cable into the USB-C port on the top of HSM10E. b) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. c) Wait for HSM10E to boot and confirm the device is in Secure Transport Mode (STM). d) Verify the displayed HSM serial number on the screen matches 712477. <p>HSM10E: Serial # 712477</p>		

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

Step	Activity	Initials	Time
<p>3.82</p>	<p>Using the Commands terminal window, CA executes the following steps to recover the HSM from STM:</p> <ol style="list-style-type: none"> Launch the LunaCM application: <code>lunacm</code> Select the HSM10E: Serial # 712477 admin partition slot: <code>slot set -s 4</code> 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.  <p>Screenshot of HSM10E STM placement during AT Ceremony 53-2 2024-03-27</p> <ol style="list-style-type: none"> 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 Recover HSM10E from STM: <code>stm recover -randomuserstring 4xp5-WtJx-THSP-A46W</code> Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step. 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 Once the string is verified type <code>proceed</code>, then press enter to recover HSM10E from STM. 		

Register HSM10E (Tier 7) Audit Credentials

Step	Activity	Initials	Time
3.83	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Initialize the audit role: <code>role init -name au</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the HSM10E touchscreen to register a 3 of 7 audit credential set: Note: If the HSM10E touchscreen is off, tap it once to activate the display. d) When "Register your Auditor..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected audit iKey, then press continue. 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. 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. h) When HSM10E returns to its dashboard, remove the last iKey of the audit set. <p>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 92.</p>		

Configure HSM10E (Tier 7) Audit Settings

Step	Activity	Initials	Time
3.84	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ol style="list-style-type: none"> Log in with the audit role: <code>role login -name au</code> 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. When "Please ensure an iKey is inserted" is displayed, insert a randomly selected audit iKey, then press continue. When "Please insert iKey 2 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When "Please insert iKey 3 of 3" is displayed, remove the previous iKey and insert a different randomly selected audit iKey, then press continue. When HSM10E returns to its dashboard, remove the last iKey of the audit set. Using the LunaCM terminal, synchronize the HSM's clock with the host time: <code>audit time sync</code> Set the filepath where log files are written: <code>audit config path /media/HSMFD/HSM10E</code> Set audit logging configuration: <code>audit config evmask all,failure,success</code> Type <code>proceed</code>, then press enter to continue. Set audit logging rotation interval: <code>audit config interval hourly@00</code> Set audit logging maximum log file size: <code>audit config size 4096k</code> Show the audit logging configuration: <code>audit config get</code> Confirm with IW the output of the logging configuration matches with the list below: <pre> 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 </pre> <p>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 92.</p>		

Initialize HSM10E (Tier 7) Administrative Partition

Step	Activity	Initials	Time
3.85	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Initialize the HSM10E administrative partition: <code>hsm init -label HSM10E -iped</code> b) Type proceed, then press enter to continue. c) Follow the instructions on the HSM10E touchscreen to register a 3 of 7 SO and 5 of 7 domain credential set: Note: If the HSM10E touchscreen is off, tap it once to activate the display. d) When "Register your Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. e) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. i) When "Please insert iKey 2 of 3" is displayed, remove the previous iKey, insert a different randomly selected SO iKey, then press continue. 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. k) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. l) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. q) When HSM10E returns to its dashboard, remove the last iKey of the domain set. <p>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 92.</p>		

Configure HSM10E (Tier 7) Global Policies

Step	Activity	Initials	Time
3.86	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the HSM10E admin partition slot number: <code>slot list</code> b) Select the HSM10E admin partition slot: <code>slot set -s 4</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the HSM10E touchscreen to perform SO authentication: Note: If the HSM10E touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When HSM10E returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, activate FIPS mode: <code>hsm changeHP -policy 12 -value 0</code> j) Type <code>proceed</code>, then press enter to continue. k) Disable PIN change after setup: <code>hsm changeHP -policy 21 -value 0</code> l) Verify HSM10E is in FIPS approved operation mode: <code>hsm showinfo</code> <p>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 92.</p>		

Create HSM10E (Tier 7) Application Partition

Step	Activity	Initials	Time
3.87	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ol style="list-style-type: none"> a) Create the partition: <code>partition create</code> b) Verify the application partition slot number: <code>slot list</code> c) Select the application partition slot: <code>slot set -s 3</code> d) Initialize the application partition: <code>partition init -label HSM10E_KSK-2024</code> e) Type proceed, then press enter to continue. f) Follow the instructions on the HSM10E touchscreen to register the SO and domain credential sets: Note: If the HSM10E touchscreen is off, tap it once to activate the display. g) When "Register your Partition Security Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. h) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. k) When "Please ensure an iKey is inserted" is displayed, leave the current iKey inserted, then press continue. 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. 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. n) When "Set up your domain..." is displayed, remove the last iKey from the previous set, select "Join existing domain", then press continue. o) When "Please insert first iKey" is displayed, insert a randomly selected domain iKey, then press continue. 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. 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. 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. 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. t) When HSM10E returns to its dashboard, remove the last iKey of the domain set. <p>Note 1: The "KE-CL" displayed on the dashboard indicates Key Export and Cloning are enabled.</p> <p>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 92.</p>		

Configure HSM10E (Tier 7) Partition Policies

Step	Activity	Initials	Time
3.88	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Log in as the Partition Officer: <code>role login -name po</code> b) Follow the instructions on the HSM10E touchscreen to perform Partition SO authentication: Note: If the HSM10E touchscreen is off, tap it once to activate the display. c) When "Please insert first iKey" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. f) When HSM10E returns to its dashboard, remove the last iKey of the SO set. g) Using the LunaCM terminal, allow partition activation with PIN: <code>partition changepolicy -policy 22 -value 1</code> <p>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 92.</p>		

Register HSM10E (Tier 7) CO Credentials and PIN

Step	Activity	Initials	Time
3.89	<p>Using the LunaCM terminal, CA executes the following steps:</p> <p>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.</p> <ul style="list-style-type: none"> a) Initialize the CO role: <code>role init -name co</code> b) Follow the instructions on the HSM10E touchscreen to register a 3 of 7 CO credential set: Note: If the HSM10E touchscreen is off, tap it once to activate the display. c) When "Register your Crypto Officer..." is displayed, select "Use existing quorum of iKeys", then press continue. d) When "Please insert first iKey" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. g) When HSM10E returns to its dashboard, remove the last iKey of the CO set. h) Using the LunaCM terminal, configure a CO PIN: <code>role createchallenge -name co</code> i) When "Enter new challenge secret:" is displayed, type 11223344, then press enter. j) When "Re-enter new challenge secret:" is displayed, type 11223344, then press enter. k) Log out of CO role: <code>role logout</code> <p>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 92.</p>		

Restore the KSK Key Pair to HSM10E (Tier 7)

Step	Activity	Initials	Time
3.90	<p>Using the LunaCM terminal, CA executes the following steps to restore the KSK key pair:</p> <p>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.</p> <ul style="list-style-type: none"> a) Log in with the Crypto Officer role: <code>role login -name co</code> b) When "enter password" is displayed, enter the secret password: 11223344 c) Follow the instructions on the HSM10E touchscreen to perform CO authentication: Note: If the HSM10E touchscreen is off, tap it once to activate the display. d) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. g) When HSM10E returns to its dashboard, remove the last iKey of the CO set. h) Verify the BHSM2W admin partition slot number: <code>slot list</code> i) List the backups in BHSM2W by specifying BHSM2W's slot number: <code>partition archive list -slot 105</code> j) List the content of the backups in BHSM2W: <code>partition archive contents -slot 105 -partition KSK-2024</code> k) Follow the instructions on the BHSM2W touchscreen to perform CO authentication: Note: If the HSM10E touchscreen is off, tap it once to activate the display. l) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected CO iKey, then press continue. 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. 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. o) When BHSM2W returns to its dashboard, remove the last iKey of the CO set. <p style="text-align: right;"><i>Continued on next page</i></p>		

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

Step	Activity	Initials	Time
3.91	<p>Using the LunaCM terminal, CA executes the following steps to restore the KSK key pair:</p> <ul style="list-style-type: none"> a) Initiate the restore from BHSM2W to HSM10E: <code>partition archive restore -slot 105 -partition KSK-2024</code> b) Follow the instructions on the BHSM2W touchscreen to perform CO 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 CO iKey, then press continue. 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. 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. f) When BHSM2W returns to its dashboard, remove the last iKey of the CO set. g) Display the KSK key pair on HSM10E: <code>partition contents</code> h) Match the displayed KSK label with the key label indicated on step 3.27 		

Verify KSK Key Pair in HSM10E (Tier 7)

Step	Activity	Initials	Time
3.92	<p>Using the LunaCM, then Commands terminal, CA executes the following steps to verify the KSK key pair:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: <code>exit</code> b) Using the Commands terminal window, verify the presence of the keypair created previously: <code>kskm-keymaster --hsm luna inventory</code> c) Match the displayed KSK label with the key label indicated on step 3.27 d) Execute the command below to change the working directory: <code>cd /media/HSMFD</code> e) launch LunaCM: <code>lunacm</code> 		

Place BHS2W (Tier 7) into Secure Transport Mode (STM)

Step	Activity	Initials	Time
3.93	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the admin partition slot number: <code>slot list</code> b) Select the BHS2W application partition slot: <code>slot set -s 105</code> c) Log in with the Security Officer role: <code>role login -name so</code> d) Follow the instructions on the BHS2W touchscreen to perform SO authentication: Note: If the BHS2W touchscreen is off, tap it once to activate the display. e) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. h) When BHS2W returns to its dashboard, remove the last iKey of the SO set. i) Using the LunaCM terminal, place BHS2W into STM: <code>stm transport</code> j) Type <code>proceed</code>, then press enter to continue. k) Verify the BHS2W dashboard indicates the device is in Secure Transport Mode and the random and verification strings are displayed in the terminal window. 		

Print BHS2W Secure Transport Mode (STM) Strings

Step	Activity	Initials	Time
3.94	<p>CA executes the following steps:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: <code>exit</code> b) Using the Commands terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot): <code>echo BHS2W</code> c) Print two copies of the STM strings, then verify the screenshot: <code>screencap-verify</code> Note: One copy for the audit bundle and one copy for the BHS2W TEB. d) Upon successful verification of the screenshot, close the image viewer application. 		

Place BHSM2W (Tier 7) in the TEB

Step	Activity	Initials	Time
3.95	<p>CA performs the following steps to prepare BHSM2W for storage:</p> <ul style="list-style-type: none"> a) Unplug the HSM cable from the upper USB-C port of BHSM2W. 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. c) Read aloud the HSM serial number while the IW verifies it matches the information below. d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. e) Give IW the sealing strips for post-ceremony inventory. f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. g) Initial the TEB along with IW using a ballpoint pen. h) Call RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. i) Give RKOS the TEB. <p>BHSM2W: TEB # BB02639619 / Serial # 718018</p>		

Launch LunaCM

Step	Activity	Initials	Time
3.96	<p>CA executes the following steps to launch LunaCM:</p> <pre>lunacm</pre>		

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

Step	Activity	Initials	Time
3.97	<p>Using the LunaCM terminal, CA executes the following steps:</p> <ul style="list-style-type: none"> a) Verify the admin partition slot number: <code>slot list</code> b) Select the HSM10E application partition slot: <code>slot set -s 3</code> c) Deactivate the CO role: <code>role deactivate -name co</code> d) Select the HSM10E admin partition slot: <code>slot set -s 4</code> e) Log in with the Security Officer role: <code>role login -name so</code> f) Follow the instructions on the HSM10E touchscreen to perform SO authentication: Note: If the HSM10E touchscreen is off, tap it once to activate the display. g) When "Please ensure an iKey is inserted" is displayed, insert a randomly selected SO iKey, then press continue. 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. 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. j) When HSM10E returns to its dashboard, remove the last iKey of the SO set. k) Using the LunaCM terminal, place HSM10E into STM: <code>stm transport</code> l) Type <code>proceed</code>, then press enter to continue. 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. 		

Print HSM10E Secure Transport Mode (STM) Strings

Step	Activity	Initials	Time
3.98	<p>CA executes the following steps:</p> <ul style="list-style-type: none"> a) Exit the LunaCM terminal window by typing the following command: <code>exit</code> b) Using the Commands terminal window, transcribe the HSM's label for chain of custody tracking. (It will be included in the screenshot): <code>echo HSM10E</code> c) Print two copies of the STM strings, then verify the screenshot: <code>screencap-verify</code> Note: One copy for the audit bundle and one copy for the HSM10E TEB. d) Upon successful verification of the screenshot, close the image viewer application. 		

Place HSM10E (Tier 7) in the TEB

Step	Activity	Initials	Time
3.99	<p>CA performs the following steps to prepare HSM10E for storage:</p> <ul style="list-style-type: none"> a) Unplug the HSM cable from the upper USB-C port of HSM10E. 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. c) Read aloud the HSM serial number while the IW verifies it matches the information below. d) Place the HSM and 1 sheet of paper with the printed STM strings into its designated new TEB, then seal it. e) Give IW the sealing strips for post-ceremony inventory. f) Place the HSM onto its designated space on the ceremony table visible to the audit camera. g) Initial the TEB along with IW using a ballpoint pen. h) Place the HSM TEB on the cart. <p>HSM10E: TEB # BB02639623 / Serial # 712477</p>		

Ceremony Break

Step	Activity	Initials	Time
3.100	<p>CA divides the participants who desire a ceremony break into groups and ensures the following:</p> <ul style="list-style-type: none"> a) Remaining participants are sufficient to maintain dual occupancy guidelines for the ceremony room. b) Audit Cameras are never obstructed. c) Live stream audio is muted until the ceremony resumes. <p>RKOS will escort each group of participants out of the ceremony room for the ceremony break.</p>		
3.101	<p>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.</p>		

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	<p>CA performs the following steps to stop logging:</p> <p>a) Execute the command below using the Commands terminal window to stop logging the terminal session: <code>exit</code></p> <p>Note: The Commands terminal session window will remain open.</p> <p>b) Disconnect the USB HSM cables from the laptop.</p>		

Print Logging Information

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

Prepare Blank FDs and Copy the HSMFD Contents

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

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: a) <code>cd /tmp</code> b) <code>umount /media/HSMFD</code> CA removes the HSMFD, then places it on the holder. Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.		
4.7	CA performs the following steps to shut down the laptop: a) Power OFF the laptop by pressing the power button. b) Disconnect all connections from the laptop. c) Remove the OS media from the laptop, and place it in its case. d) Close all laptop latches.		
4.8	CA performs the following steps to prepare the OS media bundle for storage: 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. b) Place 2 HSMFDs and 2 OS media SD cards into a plastic card case. 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. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS media bundle onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the OS media bundle TEB on the cart. OS Media (release coen-1.1.0) + HSMFD: TEB # BB02639625		
4.9	CA performs the following steps to prepare the KMF-West HSMFD bundle for transport: 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. b) Place 2 HSMFDS into a plastic card case. 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. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSMFD bundle onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Call RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. h) Give RKOS the TEB. KMF West Transport HSMFD TEB # BB02639627		
4.10	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).		

Place Laptop4 into a TEB

Step	Activity	Initials	Time
4.11	<p>CA performs the following steps to prepare the Laptop for storage:</p> <ul style="list-style-type: none"> 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. b) Read aloud the service tag number from the bottom of the laptop while the IW verifies it matches the information below. c) Place the Laptop into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the Laptop onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the Laptop TEB on the cart. <p>Laptop4: TEB # BB81420050 / Service Tag # 58SVSG2</p>		

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

Step	Activity	Initials	Time
4.12	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
4.13	<p>SSC1 opens Safe #1 while shielding the combination from the camera.</p> <p>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.</p>		
4.14	<p>SSC1 removes the safe log, writes the date and time, then signs the safe log where "Open Safe" is indicated.</p> <p>IW verifies this entry, then initials it.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p>		
4.15	<p>CA performs the following steps to return each piece of equipment to the safe:</p> <ul style="list-style-type: none"> a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number, then verify its integrity. c) Present the equipment TEB to the audit camera above, then place it inside Safe #1 (Equipment Safe). d) Write the date, time, and signature on the safe log where "Return" is indicated. e) IW verifies the safe log entry, then initials it. <p>HSM9E: TEB # BB02639624 BHSM1E: TEB # BB02639622 BHSM2E: TEB # BB02639621 HSM10E: TEB # BB02639623 Laptop4: TEB # BB81420050 OS media (release coen-1.1.0) + HSMFD: TEB # BB02639625</p> <p>Note: The shelves in the equipment safe can slide in and out for ease of use.</p>		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
4.16	SSC1 writes the date and time, then signs the safe log where " Close Safe " is indicated. IW verifies the entry, then initials it.		
4.17	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.		
4.18	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).		

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
4.19	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)		
4.20	SSC2 opens Safe #2 while shielding the combination from the camera. 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.		
4.21	SSC2 removes the safe log, writes the date and time, then signs the safe log where " Open Safe " is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		

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

Step	Activity	Initials	Time
4.22	<p>COs perform the following steps sequentially to place the listed TEBs:</p> <ol style="list-style-type: none"> CO reads aloud the TEB number, verifies integrity of TEB, then presents it to the audit camera above. CO announces their box number, then CA operates the guard key in that box's lower lock with the key blade facing downward. CO operates their tenant key in that box's upper lock with the key blade facing upward, then opens the safe deposit box. CO places their TEB(s) in their safe deposit box, locks it, then removes their key. CO writes the date and time, then signs the safe log where "Place" is indicated. IW verifies the completed safe log entry, then initials it. CA locks the safe deposit box, then removes the guard key. <p>CO1: Frederico Neves Box # 1239 CO and SO TEB # BB02639650 Audit and Domain TEB # BB02639649</p> <p>CO2: Pia Gruvö Box # 1264 CO and SO TEB # BB02639648 Audit and Domain TEB # BB02639647</p> <p>CO3: Ondrej Filip Box # 1241 CO and SO TEB # BB02639646 Audit and Domain TEB # BB02639645</p> <p>CO4: Robert Seastrom Box # 1243 CO and SO TEB # BB02639644 Audit and Domain TEB # BB02639643</p> <p>CO5: Nomsa Mwayenga Box # 1262 CO and SO TEB # BB02639642 Audit and Domain TEB # BB02639641</p> <p>CO6: Hugo Salgado Box # 1242 CO and SO TEB # BB02639640 Audit and Domain TEB # BB02639639</p> <p>CO7: Dileepa Lathsara Box # 1263 CO and SO TEB # BB02639638 Audit and Domain TEB # BB02639637</p>		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
4.23	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.		
4.24	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.		
4.25	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).		

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.		
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. All in-person attendees may sign to attest the Root KSK 2024 generation output log.		
5.3	CA reviews IW's script, then signs the participants list.		
5.4	IW signs the list and records the completion time.		

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.		
5.6	CA instructs the SA to stop the audit camera video recording.		
5.7	CA informs onsite participants of post ceremony activities.		
5.8	Ceremony participants take a group photo.		

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 94.

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 95.

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 96. 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 __

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:

Signature:

Date: 2024 Apr __

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:

Signature:

Date: 2024 Apr __