RS

Root DNSSEC KSK Ceremony 59

Thursday 13 November 2025

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 8th Edition (2025-04-14)

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	Paul Hoffman / ICANN		2025 Nov —	
IW	Patrick Jones / ICANN			
SSC1	Rob Hoggarth / ICANN			
SSC2	Daniel Gluck / ICANN			
CO1	George Michaelson			
CO2	Pia Gruvö			
CO3	Ondřej Filip			
CO4 Current	Robert Seastrom			
CO4 Successor	Lodrina Cherne			
CO6	Hugo Salgado			
CO7	Dileepa Lathsara			
RZM	Trevor Davis / Verisign			
AUD	Elyana Furman / RSM			
AUD	Matthew Skipper / RSM			
SA	Eduardo Corzo / ICANN			
SA	Sean Freeark / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Giose McGinty			
SW	Ryan Covietz			
EW	Aurelien Derouineau			
EW	Clayton Calvert			
EW	Deb Cooley			

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

Table of Contents

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 SSCs and COs into Tier 5 (Safe Room) to retrieve required materials from the following locations:

- Safe #1 containing all equipment: HSMs, laptops, OS media, etc
- Safe #2 containing all credentials: Crypto Officer credentials are required to operate HSMs

Initiate and Summarize the Ceremony

Step	Activity	Initials	Time
1.1	CA confirms with SA that all audit cameras are recording and online video streaming is active.		1800
1.2	CA welcomes all in-person and remote participants to Root DNSSEC KSK Ceremony 59 on Thursday 13 November 2025 and summarizes the purpose of the ceremony.		1805
1.3	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.		1807
1.4	CA asks that any first-time ceremony participants in the room introduce themselves.		1809

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
1.5	CA reviews emergency evacuation procedures with onsite participants.		1809
1.6	CA explains the use of personal electronic devices during the ceremony.		1809

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) within +/- 15 seconds: Date and time: 20251113T1810 **Note: All entries into this script or any logs should follow this common source of time.**		1810

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1.8	CA transports the guard key and flashlight, and with IW escorts SSC2 and the COs into Tier 5 (Safe Room.)		1812
1.9	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.**		1813
1.10	Perform the following steps to update the safe log: A) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. B) IW provides the safe log printout to SSC2. C) SSC2 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. D) IW verifies the entry, then initials it.		1814

COs Access the Credentials in Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
1.11	COs perform the following steps sequentially to access the listed TEBs: A) CO announces their box number, then CA operates the **guard key** in that box's **lower lock** with the key blade facing **downward**. B) CO operates their **tenant key** in that box's **upper lock** with the key blade facing **upward**, then opens the safe deposit box. C) CO verifies the box's integrity, then removes the TEBs. D) CO reads aloud the TEB numbers, verifies integrity of TEBs, then presents them to the audit camera above. E) CO performs the actions specified below, locks their safe deposit box, then removes their key unless otherwise specified. **Note: CO tenant keys will remain inserted in their assigned safe deposit box lock or retrieved from a new safe deposit box when specified below.** F) CO writes the date and time, then signs the safe log. G) IW verifies the completed safe log entries, then initials them. H) CA locks the safe deposit box, then removes the guard key. **Crypto Officer 1: George Michaelson - Box # 1238** **Luna CO and SO TEB # BB02638611** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Luna Audit and Domain TEB # BB02638610** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Keyper Set #1 TEB #BB02638609** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Keyper Set #2 TEB #BB02638608** (Check/Return) - *LV: KSK Ceremony 55 2024-10-17* **Crypto Officer 2: Pia Gruvö - Box # 1264** **Luna CO and SO TEB # BB02638580** (Keep for Use) - *LV: KSK Ceremony 57 2025-04-24* **Luna Audit and Domain TEB # BB02639647** (Keep for Use) - *LV: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638606** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Keyper Set #2 TEB #BB02638579** (Check/Return) - *LV: KSK Ceremony 57 2025-04-24* **Crypto Officer 3: Ondřej Filip - Box # 1241** **Luna CO and SO TEB # BB02638578** (Keep for Use) - *LV: KSK Ceremony 57 2025-04-24* **Luna Audit and Domain TEB # BB02639645** (Keep for Use) - *LV: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638604** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Keyper Set #2 TEB #BB02638577** (Check/Return) - *LV: KSK Ceremony 57 2025-04-24* **Crypto Officer 4 Current: Robert Seastrom - Box # 1243** (Key shall remain in lock) **Luna CO and SO TEB # BB02638602** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Luna Audit and Domain TEB # BB02639643** (Keep for Use) - *LV: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638601** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Keyper Set #2 TEB #BB02639668** (Keep for Use) - *LV: KSK Ceremony 53-1 2024-04-25* **Crypto Officer 6: Hugo Salgado - Box # 1242** **Luna CO and SO TEB # BB02638574** (Keep for Use) - *LV: KSK Ceremony 57 2025-04-24* **Luna Audit and Domain TEB # BB02639639** (Keep for Use) - *LV: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638599** (Keep for Use) - *LV: KSK Ceremony 55 2024-10-17* **Keyper Set #2 TEB #BB02638573** (Check/Return) - *LV: KSK Ceremony 57 2025-04-24* **Crypto Officer 7: Dileepa Lathsara - Box # 1263** **Luna CO and SO TEB # BB02639638** (Keep for Use) - *LV: KSK Ceremony 53-2 2024-04-26* **Luna Audit and Domain TEB # BB02639637** (Keep for Use) - *LV: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02639495** (Keep for Use) - *LV: KSK Ceremony 47 2022-11-03* **Keyper Set #2 TEB #BB02639667** (Check/Return) - *LV: KSK Ceremony 53-1 2024-04-25* **Note 1: "LV=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.** **Note 2: Arrows on the safe deposit box doors indicate key type and blade direction.**		1841

EXCEPTION - Box 1241 CO3 @ 1830 had difficulty opening. After CO3 removed & verified his items, closing box tested again and failed. Box 1241 was taped open, key given to RCOS CO3 opened 1240 and placed his remaining item in it and took key for 1240.

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1.12	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 entry, then initials it.		1841
1.13	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.		1841
1.14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).		1842

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
1.15	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		1845
1.16	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.**		1846
1.17	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 safe log printout 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.		1847

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

Step	Activity	Initials	Time
1.18	CA performs the indicated action for each item listed below with the following steps: 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. **Keyper HSM5E: TEB # BB51184554 (Check/Return)** Last Verified: KSK Ceremony 53-1 2024-04-25 **Keyper HSM6E: TEB # BB51184243 (Check/Return)** Last Verified: KSK Ceremony 49 2023-04-27 **Keyper HSM7E: TEB # BB51184258 (Check/Return)** Last Verified: KSK Ceremony 57 2025-04-24 **Keyper HSM8E: TEB # BB51184584 (Place on Cart)** Last Verified: KSK Ceremony 55 2024-10-17 **Luna HSM9E: TEB # BB02638598 (Place on Cart)** Last Verified: KSK Ceremony 55 2024-10-17 **Luna HSM10E: TEB # BB02638584 (Check/Return)** Last Verified: KSK Ceremony 57 2025-04-24 **Luna BHSM1E: TEB # BB02638583 (Check/Return)** Last Verified: KSK Ceremony 57 2025-04-24 **Luna BHSM2E: TEB # BB02638582 (Check/Return)** Last Verified: KSK Ceremony 57 2025-04-24 **Luna BHSM3E: TEB # BB02638210 (Place on Cart)** Last Verified: Acceptance Testing Ceremony 59 2025-11-12 **Laptop5E: TEB # BB81420055 (Check/Return)** Last Verified: KSK Ceremony 57 2025-04-24 **Laptop6E: TEB # BB81420054 (Place on Cart)** Last Verified: Acceptance Testing Ceremony 57 2025-04-23 **OS media (release coen-2.0.1) + HSMFD: TEB # BB02638581 (Place on Cart)** Last Verified: KSK Ceremony 57 2025-04-24 **KSK-2017: TEB # BB02638662 (Check/Return)** Last Verified: KSK Ceremony 51 2023-11-30 **KSK-2023: TEB # BB02639665 (Check/Return)** Last Verified: KSK Ceremony 53-1 2024-04-25 **Note 1: "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.** **Note 2: The shelves in the equipment safe can slide in and out for ease of use.**		1853

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

Step	Activity	Initials	Time
1.19	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.		1855
1.20	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.		1855
1.21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		1856

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 Hardware Security Module Flash Drive (HSMFD)
- Start the log sessions
- Power ON the HSM (Tier 7)

Laptop6E Setup

Step	Activity	Initials	Time
2.1	CA performs the following steps to prepare each item listed below: A) Remove the TEB from the cart, then place it onto the HSM designated space of the ceremony table visible to the audit camera. B) Inspect the equipment TEB for tamper evidence. C) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the TEB number and service tag (if applicable) from the TEB. D) Remove and discard the TEB, then place the contents on its designated area of the ceremony table. **Laptop6E: TEB # BB81420054 / Service Tag # 90YDBT3** Last Verified: Acceptance Testing Ceremony 57 2025-04-23 **OS media (release coen-2.0.1) + HSMFD: TEB # BB02638581** Last Verified: KSK Ceremony 57 2025-04-24 **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.**		1902
2.2	CA performs the following steps to confirm that no hard drive and battery are in the laptop: A) Flip the laptop upside-down and place it on the HSM designated area of the ceremony table. B) Note the empty bays where the batteries and permanent storage have been previously removed.		1902

Step	Activity	Initials	Time
2.3	CA performs the following steps to boot the laptop, beginning with the laptop screen in the **CLOSED** position: A) Insert the **OS media release coen-2.0.1 Copy # 2** into the port **R2** on **right** side of the laptop. **Note: The microSD card should be inserted upside-down with the metal contacts of the microSD card visible from above.** B) Connect the USB-A Hub for flash drive connectivity to port **B3** on the **back** of the laptop, then position the hub on the **left** side of the laptop. C) Connect the USB-C cable for the AC adapter to port **L1** on the **left** side of the laptop. D) Connect the USB-A to USB-C cable for the Thales HSM to port **L2** on the **left** side of the laptop. E) Connect the USB-A to serial cable for the Keyper HSM to port **L3** on the **left** side of the laptop. F) Connect the HDMI cable for the external HDMI display to port **B1** on the **back** of the laptop. G) Connect the ethernet cable for the Keyper HSM to port **B2** on the **back** of the laptop. H) Connect the USB-C to USB-B cable for the printer to port **R1** on the **right** side of the laptop. I) Open the laptop screen, then press the power button to turn the laptop **ON**.		1907
2.4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Use **CTRL + +** and **CTRL + -** to **Zoom In** and **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**		1908

OS Media coen-2.0.1 Hash Verification

Step	Activity	Initials	Time
2.5	Using the **Commands** terminal window, CA ensures the OS media is mounted in read-only mode by executing the following command: `mount | grep /dev/mmcblk0` **Note: (ro,xxx) indicates read-only while (rw,xxx) would indicate read/write mode.**		1909

2.6	Using the **Commands** terminal window, the CA executes the following steps:
	A) Verify the byte count of the microSD card matches the **OS media release coen-2.0.1** ISO size **643692544** by running the following command:
	`df -B1 /dev/mmcblk0`
	B) Calculate the SHA-256 hash by executing:
	`head -c 643692544 /dev/mmcblk0 | sha2wordlist`
	C) CA reads aloud the PGP Wordlist of the SHA-256 hash while IW and participants confirm that the result matches.
	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.
	
	SHA-256 hash:
	78e1b1452d62b075d5658ac652ad6eeccf15a81d25d63f55b9fc983463ba91d4
	PGP Words:
	island tolerance sailboat detector button gadgetry ruffled impartial sterling glossary Oakland responsive Dupont perceptive goldfish unicorn stagehand bifocals retouch breakaway bombast speculate cowbell equipment sentence Wilmington printer confidence flatfoot puberty pheasant souvenir
	
	Note: The SHA-256 hash of the OS media release coen-2.0.1 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/59
			1910

Printer Setup

Step	Activity	Initials	Time
2.7	CA confirms that the printer is switched **ON**.		1910
2.8	Using the **Commands** terminal window, the CA executes the command below to configure the printer and print a test page: `configure-printer`		1911

Date Setup

Step	Activity	Initials	Time
2.9	Using the **Commands** terminal window, the CA executes the command below to verify the date/time reasonably matches the ceremony clock. A) `date` If the date/time do not match, perform the following steps: B) Execute `date -s "20251113 HH:MM:SS"` to set the time. **where `HH` is two-digit hour, `MM` is two-digit minutes and `SS` is two-digit seconds.** C) Execute `date` to confirm the date/time matches the clock.		1911

Connect the Ceremony 57 Hardware Security Module Flash Drive (HSMFD)

Step	Activity	Initials	Time
2.10	CA connects the **Ceremony 57 HSMFD** to port **H1** on the USB hub, 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.		1912
2.11	Using the **Commands** terminal window, the CA executes the command below to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash -c` CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script. IW confirms that the result matches the SHA-256 hash of the HSMFD using the HSMFD hash printout from the Ceremony 57 OS Media bundle. **HSMFD SHA-256 HASH** 2025/04/24 # find -P /media/HSMFD/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wordlist SHA-256: d70dc041f9bad3aca381beafcc486140086055575a75ef536d736f447d7d6660 PGP Words: stopwatch asteroid slowdown decadence waffle puberty stapler penetrate reform inventive skydive pharmacy spigot dictator fallout Dakota aimless fortitude edict Eskimo enlist impartial uncut enterprise goggles hurricane gremlin designing klaxon insincere framework fortitude		1913

Distribute Unused Ceremony 57 HSMFD

Step	Activity	Initials	Time
2.12	CA gives the unused **Ceremony 57 HSMFD** and the sheet of paper with the HSMFD hash printout to RKOS.		1914

Start the Terminal Session Logging

Step	Activity	Initials	Time

2.13	Using the **Commands** terminal window, CA performs the following steps to capture the activities of the terminal window:
	A) Change the working directory to HSMFD by executing:
	`cd /media/HSMFD`
	B) Start logging the terminal window:
	`script script-20251113.log`
			1914

Start the HSM Output Logging

Step	Activity	Initials	Time

2.14	Using the **HSM Output** terminal window, CA performs the following steps to capture the activity logs of the Keyper HSM:
	A) Change the working directory to HSMFD by executing:
	`cd /media/HSMFD`
	B) Set the serial port baud rate by executing:
	`stty -F /dev/ttyUSB0 115200`
	C) Start logging the serial output by executing:
	`ttyaudit /dev/ttyUSB0`
	Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.
			1916

Keyper HSM8E (Tier 7) Setup

Step	Activity	Initials	Time
2.15	CA performs the following steps to prepare **Keyper HSM8E**: A) Remove the TEB from the cart, then place it onto the HSM designated space of the ceremony table visible to the audit camera. B) Inspect the TEB for tamper evidence. C) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the TEB number and the serial number from the TEB. D) Remove and discard the TEB. E) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the **Keyper HSM8E** serial number located on the back. F) With RKOS assistance, place **Keyper HSM8E** on its stand in its designated area on the ceremony table. **Keyper HSM8E: TEB # BB51184584 / Serial # H2110010** ✓ **Last Verified: KSK Ceremony 55 2024-10-17**		1918

Power ON Keyper HSM8E (Tier 7)

Step	Activity	Initials	Time
2.16	CA performs the following steps to prepare **Keyper HSM8E**: A) Verify the label on the HSM reads **HSM8E**. B) Plug the null modem cable into the serial port of **Keyper HSM8E**. C) Connect the power to **Keyper HSM8E**, then switch it **ON**. **Note: Status information should appear in the HSM output terminal window.** D) Scroll up on the terminal window while IW verifies the displayed HSM serial number on the screen reads **H2110010**. E) Scroll down to the end of the terminal window. **Keyper HSM8E: Serial # H2110010** ✓ **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		1921

Luna HSM9E (Tier 7) Setup

Step	Activity	Initials	Time
2.17	CA performs the following steps to prepare **Luna HSM9E**: A) Remove the TEB from the cart, then place it onto the HSM designated space of the ceremony table visible to the audit camera. B) Inspect the TEB for tamper evidence. C) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the TEB number and the serial number from the TEB. D) Remove and discard the TEB, then remove the HSM from its plastic case. E) Place **Luna HSM9E** on its designated stand face down to allow the audit camera to record its serial number. F) Set the STM screenshot printout aside for use in forthcoming steps. G) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the **Luna HSM9E** serial number. H) Flip **Luna HSM9E** over face up in its designated stand. **Luna HSM9E: TEB # BB02638598 / Serial # 712482** ✓ **Last Verified: KSK Ceremony 55 2024-10-17**		1924

Power ON Luna HSM9E (Tier 7)

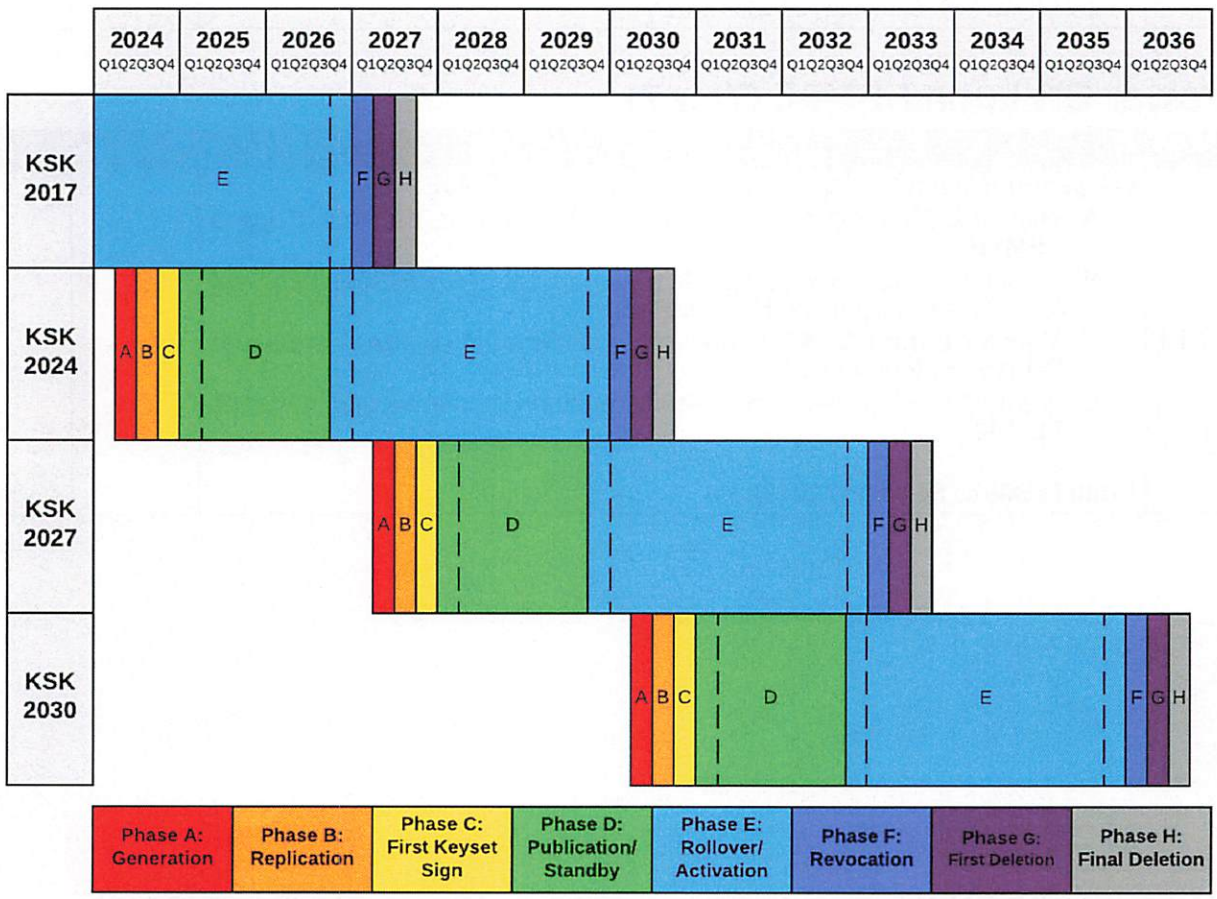
Step	Activity	Initials	Time
2.18	CA performs the following steps to prepare **Luna HSM9E**: A) Plug a USB HSM cable into the USB-C port on the **top** of **Luna HSM9E**. B) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. C) Wait for **Luna HSM9E** to boot, then confirm the device is in Secure Transport Mode (STM). D) Verify the displayed HSM serial number on the screen matches **712482**. **Luna HSM9E: Serial # 712482**		1926

Act 3: Activate HSM(s) (Tier 7) and Generate Signatures

Using the ksr signer application, the CA uses the Key Signing Requests (KSRs) in conjunction with the HSM to generate the Signed Key Responses (SKRs) by performing the steps below:

- The CA activates the HSM using the Crypto Officers' credentials
- After connectivity is confirmed, the flash drive containing the KSRs is inserted into the laptop
- The ksr signer application uses the private key stored in the HSM to generate the SKRs containing the digital signatures of the ZSK slated for future Root Zone signing
- The CA prints the signer log, backs up the newly generated SKRs, then deactivates the HSM
- There is currently a KSK rollover in progress. This is a lengthy process spanning multiple years in strict coordination between the Root Zone Manager and Root Zone Maintainer. The rollover process entails generating multiple sets of SKRs each calendar quarter to cover various scenarios. These scenarios include remaining in the current phase, proceeding to the next phase, or falling back to a previous phase. The IANA trust anchors and rollover page contains additional information: https://www.iana.org/dnssec/files

  The following graphic represents the phases of the present and future scheduled KSK rollovers.



Crypto Officer Credentials Verification

Step	Activity	Initials	Time
3.1	The CA calls each of the COs listed below sequentially to perform the following steps: A) Using the previous ceremony script where it was last used, IW verifies the information while CO reads aloud the TEB number, then CA inspects the TEB for tamper evidence. B) CO and CA open the TEB, then the CO removes the credential case to perform the action specified below. **Crypto Officer 1: George Michaelson** **Luna CO and SO TEB # BB02638611** (CO places each iKey on its designated hook of the credential stand with SET1 credentials on the outside of the hook) - *Last Verified: KSK Ceremony 55 2024-10-17* **Luna Audit and Domain TEB # BB02638610** (CO places each iKey on its designated hook of the credential stand with SET1 credentials on the outside of the hook) - *Last Verified: KSK Ceremony 55 2024-10-17* **Keyper Set #1 TEB #BB02638609** (CO places cards on Keyper card stand) - *Last Verified: KSK Ceremony 55 2024-10-17* **Crypto Officer 2: Pia Gruvö** **Luna CO and SO TEB # BB02638580** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 57 2025-04-24* **Luna Audit and Domain TEB # BB02639647** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638606** (CO places cards on Keyper card stand) - *Last Verified: KSK Ceremony 55 2024-10-17* **Crypto Officer 3: Ondřej Filip** **Luna CO and SO TEB # BB02638578** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 57 2025-04-24* **Luna Audit and Domain TEB # BB02639645** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638604** (CO places cards on Keyper card stand) - *Last Verified: KSK Ceremony 55 2024-10-17* **Crypto Officer 4 Current: Robert Seastrom** **Luna CO and SO TEB # BB02638602** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 55 2024-10-17* **Luna Audit and Domain TEB # BB02639643** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638601** (CO places cards on Keyper card stand) - *Last Verified: KSK Ceremony 55 2024-10-17* **Keyper Set #2 TEB #BB02639668** (Place the plastic case on the table for transfer to CO successor) - *Last Verified: KSK Ceremony 53-1 2024-04-25* **Crypto Officer 6: Hugo Salgado** **Luna CO and SO TEB # BB02638574** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 57 2025-04-24* **Luna Audit and Domain TEB # BB02639639** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02638599** (CO places cards on Keyper card stand) - *Last Verified: KSK Ceremony 55 2024-10-17* **Crypto Officer 7: Dileepa Lathsara** **Luna CO and SO TEB # BB02639638** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 53-2 2024-04-26* **Luna Audit and Domain TEB # BB02639637** (CO places each iKey on its designated hook of the credential stand with **SET 1** credentials on the outside of the hook) - *Last Verified: KSK Ceremony 53-2 2024-04-26* **Keyper Set #1 TEB #BB02639495** (CO places cards on Keyper card stand) - *Last Verified: KSK Ceremony 47 2022-11-03* **Note 1: 1 OP, 1 SO, 1 CO, and 1 SMK smartcard comprise each Keyper SET.** **Note 2: 2 iKeys of each type are assigned to each Crypto Officer.** **Note 3: "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.**		1946

Enable/Activate Keyper HSM8E (Tier 7)

Step	Activity	Initials	Time
	CA performs the following steps to activate **Keyper HSM8E**: A) Utilize the HSM's keyboard to scroll through the menu using < > B) Select **"1.Set Online"**, press **ENT** to confirm. C) When **"Set Online?"** is displayed, press **ENT** to confirm. D) When **"Insert Card OP #X?"** is displayed, insert a randomly selected OP card. E) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. F) When **"Remove Card?"** is displayed, remove the OP card. G) Repeat steps **D)** to **F)** for the 2nd and 3rd OP cards.		
3.2	Confirm the **"READY"** LED on **Keyper HSM8E** is **ON.** IW records which cards were used below. Each card is returned to its designated Keyper card stand after use. Set # 1 1st OP card 4 of 7 2nd OP card 6 of 7 3rd OP card 7 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **Use credentials that haven't been used previously during this ceremony when possible.** **For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.**		1950

Verify Network Connectivity Between Laptop and Keyper HSM8E

Step	Activity	Initials	Time
3.3	CA connects the ethernet cable to the **Keyper HSM8E** LAN port.		1950

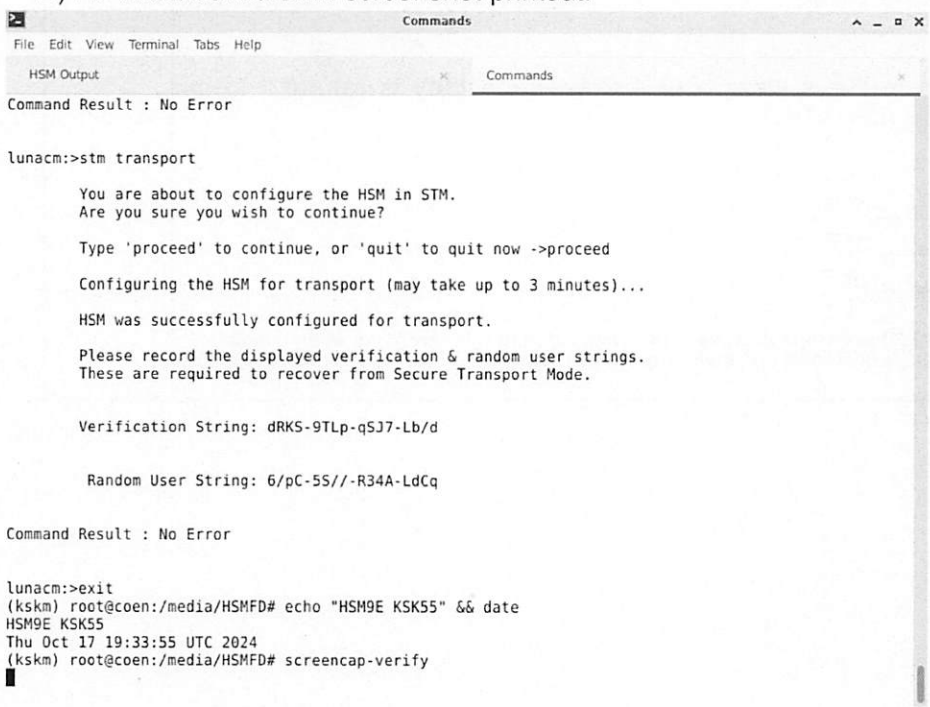
3.4	CA performs the following steps to test the network connectivity between laptop and **Keyper HSM8E**:
	A) Select the **Commands** terminal window
	B) Test connectivity by executing:
	`ping hsm`
	C) Wait for responses, then exit by pressing:
	`Ctrl + C`
			1950

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

Step	Activity	Initials	Time

3.5	Using the **Commands** terminal window, the CA executes the following steps to recover the HSM from STM:
	A) Launch the **LunaCM** application:
	`lunacm`
	B) Select the **Luna HSM9E: Serial # 712482** admin partition slot:
	`slot set -s 4`
	C) Log in with the Security Officer role:
	`role login -name so`
	D) Follow the instructions on the **Luna HSM9E touchscreen** to perform **SO** authentication:
	Note: If the Luna 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 **Luna HSM9E** returns to its dashboard, remove the last **SO** iKey.
	
	IW records which iKeys were used below. Each iKey is returned to its designated hook after use.
	
	Set # 1
	1st SO iKey 4 of 7
	2nd SO iKey 7 of 7
	3rd SO iKey 6 of 7
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.
			1952

.over Luna HSM9E (Tier 7) from Secure Transport Mode (STM) .ontinued)

Step	Activity	Initials	Time
3.6	To prepare for the next step, CA assigns half of the participants to confirm the **Random User** string from their hard copy while the other half confirm from the laptop display. Using the **LunaCM** terminal, CA executes the following steps to recover **Luna HSM9E** from STM: A) CA enters the following command, but does **NOT** press enter yet: `stm recover -randomuserstring 6/pC-5S//-R34A-LdCq` B) CA reads aloud the **Random User** string from the laptop display. When ceremony participants confirm accuracy, press **enter** to proceed. **Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.** C) CA reads aloud the **Verification** string from the laptop display while the IW confirms that the result matches the **Verification** string using the STM screenshot printout from KSK Ceremony 55 2024-10-17. D) Once the string is verified type `proceed`, then press **enter** to recover **Luna HSM9E** from STM. E) IW discards the STM screenshot printout.  **Screenshot of Luna HSM9E STM placement during KSK Ceremony 55 2024-10-17** **Note: STM strings are CaSe SeNsItIvE.**		1958

Enable/Activate Luna HSM9E (Tier 7)

Step	Activity	Initials	Time

3.7	Using the **LunaCM** terminal, CA executes the following steps to activate the Luna HSM9E:
	A) Verify the application partition slot number:
	`slot list`
	B) Select the **Luna HSM9E** application partition slot:
	`slot set -s 3`
	C) Log in with the Crypto Officer role:
	`role login -name co`
	D) When **"enter password"** is displayed, enter the **secret** password:
	`11223344`
	E) Follow the instructions on the **Luna HSM9E touchscreen** to perform **CO** authentication:
	Note: If the Luna HSM9E touchscreen is off, tap it once to activate the display.
	F) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **CO** iKey, then press continue.
	G) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue.
	H) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **CO** iKey, then press continue.
	I) When **Luna HSM9E** returns to its dashboard, remove the last **CO** iKey.
	J) Exit the **LunaCM** terminal window by typing the following command:
	`exit`
	
	IW records which iKeys were used below. Each iKey is returned to its designated hook after use.
	
	Set # 1
	1st CO iKey 2 of 7
	2nd CO iKey 3 of 7
	3rd CO iKey 1 of 7
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.
			2000

Connect the Key Signing Request Flash Drive (KSRFD)

Step	Activity	Initials	Time
3.8	CA connects the **KSRFD** to port **H3** on the USB hub, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window. **Note: The KSRFD was transferred to the facility by the RKOS. It contains 3 KSRs. The first for normal operations and the remainder for fallback scenarios.**		2001

.SR Signer for KSR 2026 Q1 Phase D to D

	Activity	Initials	Time

	.ne **Commands** terminal window, CA performs the following steps .ecute the KSR Signer:
	A) Change the working directory by executing:
	`cd /media/KSRFD/KSK59-0-D_to_D/`
	B) Sign the KSR file *ksr-root-2026-q1-0-d_to_d.xml:*
	`kskm-ksrsigner --schema publish+`
	WARNING: DO NOT CONFIRM the signing operation until instructed to proceed in a forthcoming step!
			2002

Verify the KSR Hash for KSR 2026 Q1 Phase D to D

Step	Activity	Initials	Time
3.10	When the hash of the KSR is displayed in the terminal window, perform the following: A) CA asks all Root Zone Maintainer (RZM) representatives to identify themselves. The IW verifies their government-issued identification **off camera** for the purpose of authentication while maintaining privacy. B) IW writes the RZM representative names on the following line: **Note: If no RZM representative is physically present in the room, write the representative's name and *"Remote Participant"* next to the name on the signature line.** _____ C) To prepare for the next step, the CA instructs some participants to compare the hash provided in the email sent by the RZM representative before the ceremony, while others are asked to compare the hash displayed in the terminal window. D) The CA requests that the RZM representative read aloud the SHA-256 hash of the KSR file as listed in the PGP word list while ceremony participants verify it matches. **Note: The hash and PGP word list for the KSR(s) is part of the ceremony annotated script and audit bundle.**		2005
3.11	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		2005
3.12	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The generated SKR will be located at: `/media/KSRFD/KSK59-0-D_to_D/skr-root-2026-q1-0-d_to_d.xml`		2005

Print Copies of the KSR Signer Log(s)

Step	Activity	Initials	Time
3.13	Using the **Commands** terminal window, the CA executes the commands below to print the KSR Signer log: CA presses the **tab** key to autocomplete the log file name. If multiple options are available, select the file with the highest *PID* number (i.e. the most recent). Enter the number of copies needed at the end of the command, then press Enter. `printlog kskm-ksrsigner-202511XX-pid-pid.log X` **Note: Replace "X" with the quantity of copies needed for the participants.**		2009
3.14	IW attaches a copy of the required ksr signer log to their script.		2009

Execute the KSR Signer for KSR 2026 Q1 Phase D to C

Step	Activity	Initials	Time

3.15	Using the **Commands** terminal window, CA performs the following steps to execute the KSR Signer:
	A) Change the working directory by executing:
	`cd /media/KSRFD/KSK59-1-D_to_C/`
	B) Sign the KSR file *ksr-root-2026-q1-1-d_to_c.xml:*
	`kskm-ksrsigner --schema normal`
	WARNING: DO NOT CONFIRM the signing operation until instructed to proceed in a forthcoming step!
			2010

Verify the KSR Hash for KSR 2026 Q1 Phase D to C

Step	Activity	Initials	Time
3.16	When the hash of the KSR is displayed in the terminal window, perform the following: A) To prepare for the next step, the CA instructs some participants to compare the hash provided in the email sent by the RZM representative before the ceremony, while others are asked to compare the hash displayed in the terminal window. B) The CA requests that the RZM representative read aloud the SHA-256 hash of the KSR file as listed in the PGP word list while ceremony participants verify it matches. **Note: The hash and PGP word list for the KSR(s) is part of the ceremony annotated script and audit bundle.**		2011
3.17	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		2011
3.18	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The generated SKR will be located at: `/media/KSRFD/KSK59-1-D_to_C/skr-root-2026-q1-1-d_to_c.xml`		2011

Print Copies of the KSR Signer Log(s)

Step	Activity	Initials	Time
3.19	Using the **Commands** terminal window, the CA executes the commands below to print the KSR Signer log: CA presses the **tab** key to autocomplete the log file name. If multiple options are available, select the file with the highest *PID* number (i.e. the most recent). Enter the number of copies needed at the end of the command, then press Enter. `printlog kskm-ksrsigner-202511XX-pid-pid.log X` **Note: Replace "X" with the quantity of copies needed for the participants.**		2012
3.20	IW attaches a copy of the required ksr signer log to their script.		2014

Execute the KSR Signer for KSR 2026 Q1 Phase C to C

Step	Activity	Initials	Time

3.21	Using the **Commands** terminal window, CA performs the following steps to execute the KSR Signer:
	A) Change the working directory by executing:
	`cd /media/KSRFD/KSK59-2-C_to_C/`
	B) Sign the KSR file *ksr-root-2026-q1-2-c_to_c.xml:*
	`kskm-ksrsigner --schema normal`
	WARNING: DO NOT CONFIRM the signing operation until instructed to proceed in a forthcoming step!
			2015

Verify the KSR Hash for KSR 2026 Q1 Phase C to C

Step	Activity	Initials	Time
3.22	When the hash of the KSR is displayed in the terminal window, perform the following: A) To prepare for the next step, the CA instructs some participants to compare the hash provided in the email sent by the RZM representative before the ceremony, while others are asked to compare the hash displayed in the terminal window. B) The CA requests that the RZM representative read aloud the SHA-256 hash of the KSR file as listed in the PGP word list while ceremony participants verify it matches. **Note: The hash and PGP word list for the KSR(s) is part of the ceremony annotated script and audit bundle.**		2016
3.23	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		2016
3.24	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The generated SKR will be located at: `/media/KSRFD/KSK59-2-C_to_C/skr-root-2026-q1-2-c_to_c.xml`		2016

Print Copies of the KSR Signer Log(s)

Step	Activity	Initials	Time
3.25	Using the **Commands** terminal window, the CA executes the commands below to print the KSR Signer log: CA presses the **tab** key to autocomplete the log file name. If multiple options are available, select the file with the highest *PID* number (i.e. the most recent). Enter the number of copies needed at the end of the command, then press Enter. **`printlog kskm-ksrsigner-202511XX-pid-pid.log X`** **Note: Replace "X" with the quantity of copies needed for the participants.**		2010
3.26	IW attaches a copy of the required ksr signer log to their script.		2019

Copy the Newly Generated SKR(s)

Step	Activity	Initials	Time
3.27	Using the **Commands** terminal window, the CA executes the following steps: A) Change the working directory by executing: **`cd /media/HSMFD`** B) List the contents of the KSRFD by executing: **`ls -ltrR /media/KSRFD`** C) Copy the contents of the KSRFD to the HSMFD by executing: **`cp -pR /media/KSRFD/* /media/HSMFD/`** **Note: Confirm overwrite by entering "y" if prompted.** D) List the contents of the HSMFD by executing: **`ls -ltrR`** E) Verify it has been copied successfully by executing: I) `diff -qr /media/HSMFD/KSK59-0-D_to_D/ /media/KSRFD/KSK59-0-D_to_D/` II) `diff -qr /media/HSMFD/KSK59-1-D_to_C/ /media/KSRFD/KSK59-1-D_to_C/` III) `diff -qr /media/HSMFD/KSK59-2-C_to_C/ /media/KSRFD/KSK59-2-C_to_C/` **Note: When executing a diff command, a return of no output indicates a match.** F) Unmount the KSRFD by executing: **`umount /media/KSRFD`**		2022
3.28	CA removes the **KSRFD** containing the SKR files from port **H3**, then gives it to the RZM representative. **Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.**		2022

Disable/Deactivate Keyper HSM8E (Tier 7)

Step	Activity	Initials	Time
	CA deactivates **Keyper HSM8E** by performing the following steps: A) CA selects the **HSM Output** terminal window. B) Utilize the HSM's keyboard to scroll through the menu using < > C) Select **"2.Set Offline"**, press **ENT** to confirm. D) When **"Set Offline?"** is displayed, press **ENT** to confirm. E) When **"Insert Card OP #X?"** is displayed, insert a randomly selected OP card. F) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. G) When **"Remove Card?"** is displayed, remove the OP card. H) Repeat steps **E)** to **G)** for the 2nd and 3rd OP cards.		
3.29	Confirm the **"READY"** LED on **Keyper HSM8E** is **OFF.** IW records which cards were used below. Each card is returned to its designated Keyper card stand after use. Set # 1 1st OP card 3 of 7 2nd OP card 2 of 7 3rd OP card 1 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **Use credentials that haven't been used previously during this ceremony when possible.** **For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.**		2025

Place Keyper HSM8E (Tier 7) into a TEB

Step	Activity	Initials	Time
3.30	CA switches **Keyper HSM8E** power **OFF**, then disconnects the power, serial, and ethernet connections. **Note: DO NOT unplug the cable connections on the laptop.**		2025
3.31	CA performs the following steps to prepare **Keyper HSM8E** for storage: A) IW gives the HSM's designated new TEB to the CA, then using the information below, verifies it matches while the CA reads the TEB number aloud. B) Place the HSM into its designated new TEB, then seal it. C) Give IW the sealing strips for post-ceremony inventory. D) Place the HSM onto its designated space on the ceremony table visible to the audit camera. E) Initial the TEB along with IW using a ballpoint pen. F) Place the HSM on the cart. **Keyper HSM8E: TEB # BB51184259 / Serial # H2110010**		2021

Ceremony Break

Step	Activity	Initials	Time
3.32	CA prepares for a ceremony break by performing the following steps: A) With RKOS assistance, place the credential stands containing the credentials onto the equipment cart. B) If any credentials are still in their plastic case for transfer to a successor, place the cases on the equipment cart. C) With the assistance of the IW, move the equipment cart into Tier 5 (Safe Room). Ensure both CA and IW enter Tier 5, then badge out again to return. D) Separate the participants who desire a ceremony break into two groups. The second group will go when the first group has returned. E) Ensure both groups contain sufficient personnel to maintain dual occupancy guidelines for the ceremony room. Designated personnel will escort each group of participants from, then back into the ceremony room for the ceremony break. **Note: During the break, ensure audit cameras are never obstructed and audio is muted to the livestream and local audit recording.**		2029
3.33	CA resumes the ceremony by performing the following steps: A) Once all ceremony participants have returned, retrieve the equipment cart from Tier 5 (Safe Room) with the assistance of the IW. B) With RKOS assistance, return the credential stands and credentials to their designated areas of the ceremony table. C) Ensure live stream and local recording audio is enabled. D) Perform a roll call with the attendee list.		2048

Act 4: Introduce New Backup HSM(s) (Tier 7)

Luna Backup HSMs are replaced approximately every two to three years to better ensure reliable operation of the Root Zone KSK function. Pursuant to these procedures, new Backup HSMs are periodically introduced.

The CA will introduce a new Backup HSM by performing the following steps:

- Inspect the Backup HSM's tamper evident bag for tamper evidence
- Verify new Backup HSM's serial number
- Power on the Backup HSM
- Recover Backup HSM from Secure Transport Mode (STM)
- Import credentials
- Configure Backup HSM policies
- Back up the KSK key pair
- Store the backup HSM inside of a tamper evident bag

Stop Logging the Serial Output

Step	Activity	Initials	Time
4.1	CA performs the following steps to stop logging: A) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: I) Press `Ctrl + C` II) Execute `exit` B) Disconnect the USB-A to serial cable for the Keyper HSM from port **L3** on the **left** side of the laptop. C) Connect an additional USB-A to USB-C cable for the Thales Backup HSM to port **L3** on the **left** side of the laptop. **Note: The Commands terminal session window will remain open.**		2049

HSM Log Folder Creation

Step	Activity	Initials	Time
4.2	Using the **Commands** terminal window, the CA executes the command below to create a folder for the HSM(s) logs on the HSMFD: `mkdir BHSM3E`		2050

Luna BHSM3E (Tier 7) Setup

Step	Activity	Initials	Time
4.3	CA performs the following steps to prepare **Luna BHSM3E**: A) Remove the TEB from the cart, then place it onto the HSM designated space of the ceremony table visible to the audit camera. B) Inspect the TEB for tamper evidence. C) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the TEB number and the serial number from the TEB. D) Remove and discard the TEB, then remove the HSM from its plastic case. E) Place **Luna BHSM3E** on its designated stand face down to allow the audit camera to record its serial number. F) Set the STM screenshot printout aside for use in forthcoming steps. G) Using the previous ceremony script where it was last used, IW verifies the information while CA reads aloud the **Luna BHSM3E** serial number. H) Flip **Luna BHSM3E** over face up in its designated stand. **Luna BHSM3E: TEB # BB02638210 / Serial # ~~764632~~** 764648 **Last Verified: Acceptance Testing Ceremony 59 2025-11-12**		2054

Power ON Luna BHSM3E (Tier 7)

Step	Activity	Initials	Time
4.4	CA performs the following steps to prepare **Luna BHSM3E**: A) Plug a USB HSM cable into the USB-C port on the **top** of **Luna BHSM3E**. B) Adjust the ceremony table audit camera's zoom and HSM placement on the table for optimal HSM visibility. C) Wait for **Luna BHSM3E** to boot, then confirm the device is in Secure Transport Mode (STM). D) Verify the displayed HSM serial number on the screen matches **764632**. **Luna BHSM3E: Serial # 764632**		2056

Duplicate and Distribute STM Screenshot Printout

Step	Activity	Initials	Time
4.5	Perform the following steps to prepare for STM verification: A) IW provides the STM screenshot printout from Acceptance Testing Ceremony 59 2025-11-12 to RKOS to create copies. B) RKOS creates and distributes copies for in-person participants.		2058

Recover Luna BHSM3E (Tier 7) from Secure Transport Mode (STM)

Step	Activity	Initials	Time

4.6	Using the **Commands** terminal window, the CA executes the following steps to recover the HSM from STM:
	A) Launch the **LunaCM** application:
	`lunacm`
	B) Select the **Luna BHSM3E: Serial # 764632** admin partition slot:
	`slot set -s 105`
	C) To prepare for the next step, CA assigns half of the participants to confirm the **Random User** string from their hard copy while the other half confirm from the laptop display.
	D) Using the **LunaCM** terminal, CA executes the following steps to recover **Luna BHSM3E** from STM:
	CA enters the following command, but does **NOT** press enter yet:
	`stm recover -randomuserstring XxXx-XxXx-XxXx-XxXx`
	Replace the X's with the **Random User** string from the STM screenshot printout removed from the Acceptance Testing Ceremony 59 2025-11-12 HSM TEB.
	E) CA reads aloud the **Random User** string from the laptop display. When ceremony participants confirm accuracy, press **enter** to proceed.
	Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.
	F) CA reads aloud the **Verification** string from the laptop display while the IW confirms that the result matches the **Verification** string using the STM screenshot printout from Acceptance Testing Ceremony 59 2025-11-12.
	G) Once the string is verified type `proceed`, then press **enter** to recover **Luna BHSM3E** from STM.
	H) IW discards the STM screenshot printout.
	Note: STM strings are CaSe SeNsItIvE.
			2102

Register Luna BHSM3E (Tier 7) Audit Credentials

Step	Activity	Initials	Time
4.7	Using the **LunaCM** terminal, CA executes the following steps: A) Initialize the **audit** role: `role init -name au` B) Type `proceed`, then press enter to continue. C) Follow the instructions on the **Luna BHSM3E touchscreen** to register a 3 of 7 **audit** credential set: **Note: If the Luna BHSM3E 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 **Luna BHSM3E** returns to its dashboard, remove the last **audit** iKey. IW records which iKeys were used below. Each iKey is returned to its designated hook after use. Set # 1 1st AU iKey 3 of 7 2nd AU iKey 1 of 7 3rd AU iKey 6 of 7 **Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.**		2105

Configure Luna BHSM3E (Tier 7) Audit Settings

Step	Activity	Initials	Time

4.8	Using the **LunaCM** terminal, CA executes the following steps:
	A) Log in with the audit role:
	`role login -name au`
	B) Follow the instructions on the **Luna BHSM3E touchscreen** to perform **audit** authentication:
	Note: If the Luna BHSM3E touchscreen is off, tap it once to activate the display.
	C) When **"Please ensure an iKey is inserted"** is displayed, insert a randomly selected **audit** iKey, then press continue.
	D) When **"Please insert iKey 2 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue.
	E) When **"Please insert iKey 3 of 3"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue.
	F) When **Luna BHSM3E** returns to its dashboard, remove the last **audit** iKey.
	G) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:
	`audit time sync`
	H) Set the filepath where log files are written:
	`audit config path /media/HSMFD/BHSM3E`
	I) Set audit logging configuration:
	`audit config evmask all,failure,success`
	J) Type `proceed`, then press enter to continue.
	K) Set audit logging rotation interval:
	`audit config interval hourly@00`
	L) Set audit logging maximum log file size:
	`audit config size 4096k`
	M) Show the audit logging configuration:
	`audit config get`
	N) Confirm with IW the output of the logging configuration matches with the list below:
	
	`Current Logging Configuration`
	`---------------------------`
	`event mask : Log everything`
	`rotation interval : hourly@ 0 minutes past the hour`
	`rotation size (MB): 4`
	`path to log : /media/HSMFD/BHSM3E`
	
	`Command Result : No Error`
	
	IW records which iKeys were used below. Each iKey is returned to its designated hook after use.
	
	Set # 1
	1st Audit iKey 2 of 7
	2nd Audit iKey 4 of 7
	3rd Audit iKey 7 of 7
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.
			1408

Initialize Luna BHSM3E (Tier 7) Administrative Partition

Step	Activity	Initials	Time
4.9	Using the **LunaCM** terminal, CA executes the following steps: **Note: The CA may delegate narration of this step to IW to aid concentration. Questions should be held until PED sequences finish to avoid timeout.** A) Initialize the **Luna BHSM3E** administrative partition: `hsm init -label BHSM3E -iped` B) Type `proceed`, then press enter to continue. C) Follow the instructions on the **Luna BHSM3E touchscreen** to register a 3 of 7 **SO** and 5 of 7 **domain** credential set: 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, 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 **Luna BHSM3E** returns to its dashboard, remove the last **domain** iKey. IW records which iKeys were used below. Each iKey is returned to its designated hook after use. Set # 1 1st SO iKey 6 of 7 | 1st Domain iKey 4 of 7 2nd SO iKey 7 of 7 | 2nd Domain iKey 3 of 7 3rd SO iKey 3 of 7 | 3rd Domain iKey 6 of 7 2nd SO iKey 2 of 7 | 4th Domain iKey 7 of 7 3rd SO iKey 1 of 7 | 5th Domain iKey 1 of 7 **Note: Use credentials that haven't been used previously during this ceremony when possible.** **For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.**		21 12

Configure Luna BHSM3E (Tier 7) Global Policies

Step	Activity	Initials	Time

4.10	Using the **LunaCM** terminal, CA executes the following steps:
	A) Verify the **Luna BHSM3E** admin partition slot number:
	`slot list`
	B) Select the **Luna BHSM3E** admin partition slot:
	`slot set -s 105`
	C) Log in with the Security Officer role:
	`role login -name so`
	D) Follow the instructions on the **Luna BHSM3E touchscreen** to perform **SO** authentication:
	Note: If the Luna BHSM3E 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 **Luna BHSM3E** returns to its dashboard, remove the last **SO** iKey.
	I) Using the **LunaCM** terminal, activate FIPS mode:
	`hsm changehsmpolicy -policy 55 -value 1`
	J) Verify **Luna BHSM3E** is in FIPS approved operation mode:
	`hsm showinfo`
	
	IW records which iKeys were used below. Each iKey is returned to its designated hook after use.
	
	Set # 1
	1st SO iKey 4 of 7
	2nd SO iKey 5 of 7
	3rd SO iKey 6 of 7
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.
			2115

Back Up KSK Key Pair to Luna BHSM3E (Tier 7) 1/3

Step	Activity	Initials	Time

4.11	Using the **LunaCM** terminal, CA executes the following steps to perform **CO** authentication:
	A) Verify the application partition slot number:
	`slot list`
	B) Select the HSM's application partition slot:
	`slot set -s 3`
	C) Log in with the Crypto Officer role:
	`role login -name co`
	D) When **"enter password"** is displayed, enter the **secret** password:
	`11223344`
	E) Show the KSK key pair:
	`partition contents`
	F) Match the displayed KSK label with the key label **Kmyv6jo**
			2/16

Back Up KSK Key Pair to Luna BHSM3E (Tier 7) 2/3

Step	Activity	Initials	Time
4.12	Using the **LunaCM** terminal, CA executes the following steps to back up KSK key pair: **Note: The CA may delegate narration of this step to RKOS to aid concentration. Questions should be held until PED sequences finish to avoid timeout.** A) Initiate the backup from the HSM application partition to **Luna BHSM3E**: `partition archive backup -slot 105 -partition KSK-2024` B) Follow the instructions on the **Luna BHSM3E touchscreen** to register and authenticate **SO**, Partition **SO**, **domain**, and **CO** credential sets: **Note: If the Luna BHSM3E 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. IW records which iKeys were used below. Each iKey is returned to its designated hook after use. Set # 1 1st SO iKey 6 of 7 2nd SO iKey 4 of 7 3rd SO iKey 3 of 7 2nd SO iKey 2 of 7 3rd SO iKey 1 of 7 2nd SO iKey 5 of 7 3rd SO iKey ____ of 7 **Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.**		2:19

Back Up KSK Key Pair to Luna BHSM3E (Tier 7) 2/3 (Continued)

Step	Activity	Initials	Time
4.13	A) When **"Set up your domain..."** is displayed, remove the last iKey, 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, 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 **Luna BHSM3E** returns to its dashboard, remove the last **CO** iKey. IW records which iKeys were used below. Each iKey is returned to its designated hook after use. Set # 1 1st Domain iKey 1 of 7 | 1st SO iKey 2 of 7 | 1st CO iKey 4 of 7 2nd Domain iKey 3 of 7 | 2nd SO iKey 7 of 7 | 2nd CO iKey 3 of 7 3rd Domain iKey 6 of 7 | 3rd SO iKey 6 of 7 | 3rd CO iKey 2 of 7 4th Domain iKey 4 of 7 | 2nd CO iKey 1 of 7 5th Domain iKey 2 of 7 | 3rd CO iKey 7 of 7 **Note: Use credentials that haven't been used previously during this ceremony when possible.** **For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.**		2122

Back Up KSK Key Pair to Luna BHSM3E (Tier 7) 3/3

Step	Activity	Initials	Time

4.14	Using the **LunaCM** terminal, CA executes the following steps to verify the KSK key pair:
	A) List the backups in **Luna BHSM3E** by specifying **Luna BHSM3E's** slot number:
	`partition archive list -slot 105`
	B) List the contents of the backups in **Luna BHSM3E**:
	`partition archive contents -slot 105 -partition KSK-2024`
	C) Follow the instructions on the **Luna BHSM3E touchscreen** to perform **CO** authentication:
	Note: If the Luna BHSM3E 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 **Luna BHSM3E** returns to its dashboard, remove the last **CO** iKey.
	H) Match the displayed KSK label with the key label **Kmyv6jo**
	I) Exit the **LunaCM** terminal window by typing the following command:
	`exit`
	
	IW records which iKeys were used below. Each iKey is returned to its designated hook after use.
	
	Set # 1
	1st CO iKey 1 of 7
	2nd CO iKey 3 of 7
	3rd CO iKey 2 of 7
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.
			2124

Place Luna BHSM3E (Tier 7) in the TEB

Step	Activity	Initials	Time
4.15	CA performs the following steps to prepare **Luna BHSM3E** for storage: A) Unplug the HSM cable from the upper USB-C port of **Luna BHSM3E**. B) Flip **Luna BHSM3E** over face down in its designated HSM stand. C) Using the information below, IW verifies it matches while the CA reads the HSM serial number aloud from the back. D) IW gives the HSM's designated new TEB to the CA, then using the information below, verifies it matches while the CA reads the TEB number aloud. E) Place the HSM into a plastic case. F) Place the plastic case containing the HSM into its designated new TEB, then seal it. G) Give IW the sealing strips for post-ceremony inventory. H) Place the HSM onto its designated space on the ceremony table visible to the audit camera. I) Initial the TEB along with IW using a ballpoint pen. J) Place the HSM's TEB on the cart. **Luna BHSM3E: TEB # BB02638206 / Serial # ~~764632~~** 764648		2127

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

Step	Activity	Initials	Time

4.16	Using the **Commands** terminal window, the CA executes the following steps to place the Luna HSM9E into STM:
	A) Launch the **LunaCM** application:
	`lunacm`
	B) Select the **Luna HSM9E** application partition slot:
	`slot set -s 3`
	C) Deactivate the **CO** role:
	`role deactivate -name co`
	D) Select the **Luna HSM9E** admin partition slot:
	`slot set -s 4`
	E) Log in with the Security Officer role:
	`role login -name so`
	F) Follow the instructions on the **Luna HSM9E touchscreen** to perform **SO** authentication:
	Note: If the Luna 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 **Luna HSM9E** returns to its dashboard, remove the last **SO** iKey.
	K) Using the **LunaCM** terminal, place **Luna HSM9E** into STM:
	`stm transport`
	L) Type `proceed`, then press enter to continue.
	Note: This will take approximately 3 minutes to process.
	M) Verify the **Luna HSM9E** dashboard indicates the device is in **Secure Transport Mode** and the random and verification strings are displayed in the terminal window.
	
	IW records which iKeys were used below. Each iKey is returned to its designated hook after use.
	
	Set # 1
	1st SO iKey 4 of 7
	2nd SO iKey 1 of 7
	3rd SO iKey 2 of 7
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A: Glossary number [13] and [14] on page 54.
			2133

Print Luna HSM9E Secure Transport Mode (STM) Strings

Step	Activity	Initials	Time

4.17	CA executes the following steps:
	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 KSK59" && date`
	C) To ensure the STM information prints on a single page in the forthcoming step, CA presses the following keys to return the terminal to the default zoom level:
	Use **CTRL + 0**
	D) Print two copies of the STM strings then verify the screenshot by typing the following command:
	`screencap-verify`
	Note: One copy for the audit bundle and one copy for the Luna HSM9E TEB.
	E) Upon successful verification of the printouts, close the image viewer application.
	F) CA may adjust the zoom levels again with the following commands:
	Use **CTRL + +** and **CTRL + -** to **Zoom In** and **Zoom Out**
			2134

Place Luna HSM9E (Tier 7) in the TEB

Step	Activity	Initials	Time
4.18	CA performs the following steps to prepare **Luna HSM9E** for storage: A) Unplug the HSM cable from the upper USB-C port of **Luna HSM9E**. B) Flip **Luna HSM9E** over face down in its designated HSM stand. C) Using the information below, IW verifies it matches while the CA reads the HSM serial number aloud from the back. D) IW gives the HSM's designated new TEB to the CA, then using the information below, verifies it matches while the CA reads the TEB number aloud. E) Place the HSM into a plastic case. F) Place the plastic case containing the HSM and 1 copy of the STM screenshot printout into its designated new TEB, then seal it. G) Give IW the sealing strips for post-ceremony inventory. H) Place the HSM onto its designated space on the ceremony table visible to the audit camera. I) Initial the TEB along with IW using a ballpoint pen. J) Place the HSM's TEB on the cart. **Luna HSM9E: TEB # BB02638207 / Serial # 712482** ✓		2137

OS Media coen-2.0.1 Hash Verification

Step	Activity	Initials	Time

4.19	Using the **Commands** terminal window, the CA executes the following steps:
	A) Verify the byte count of the microSD card matches the **OS media release coen-2.0.1** ISO size **643692544** by running the following command:
	`df -B1 /dev/mmcblk0`
	B) Calculate the SHA-256 hash by executing:
	`head -c 643692544 /dev/mmcblk0 | sha2wordlist`
	C) CA reads aloud the PGP Wordlist of the SHA-256 hash while IW and participants confirm that the result matches.
	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.
	
	SHA-256 hash:
	78e1b1452d62b075d5658ac652ad6eeccf15a81d25d63f55b9fc983463ba91d4
	PGP Words:
	island tolerance sailboat detector button gadgetry ruffled impartial sterling glossary Oakland responsive Dupont perceptive goldfish unicorn stagehand bifocals retouch breakaway bombast speculate cowbell equipment sentence Wilmington printer confidence flatfoot puberty pheasant souvenir
	
	Note 1: The SHA-256 hash of the OS media is being calculated a second time to ensure the contents of the microSD card have not been modified during the previous steps.
	Note 2: The SHA-256 hash of the OS media release coen-2.0.1 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/59
			2130

Act 5: Secure Hardware

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

- Copy the Hardware Security Module Flash Drive (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 return Crypto Officers' credentials to Safe #2

Stop Logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
5.1	CA performs the following steps to stop logging: A) Execute the command below using the **Commands** terminal window to stop logging the terminal session: `exit` **Note: The Commands terminal session window will remain open.**		2#39

Print Logging Information

Step	Activity	Initials	Time
5.2	CA executes the following commands to print a copy of the logging information: A) `print-script script-202511*.log` B) `print-ttyaudit ttyaudit-tty*-202511*.log` Attach the printout to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**		2#43

Prepare Blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
5.3	CA executes the command below to display the contents of the HSMFD: `ls -ltrR`		2#43
5.4	CA executes the following command to print **two** copies of the hash for the HSMFD content: `hsmfd-hash -p` **Note: One copy for the audit bundle and one copy for the OS media TEB.**		2#43
5.5	CA executes the command below, then follows the interactive prompts in the terminal window to create **five** HSMFDs copies. When prompted by the script, CA connects blank FDs labeled HSMFD to port **H4** on the USB hub: `copy-hsmfd` **Note 1: Wait for the activity light on the copied HSMFD to stop flashing before removal.** **Note 2: "copy-hsmfd -v" can be used to activate verbose mode.**		2#49

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
5.6	Using the **Commands** terminal window, the CA executes the commands below to unmount the HSMFD: A) `cd /tmp` B) `umount /media/HSMFD` CA removes the HSMFD from port **H1**, then places it on the holder. **Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.**		2150
5.7	CA performs the following steps to shut down the laptop: A) Power **OFF** the laptop by pressing the power button, then clicking **Shut Down** on the pop up window. B) Disconnect all connections from the laptop. C) Return applicable cables and accessories to IW. D) Remove the OS media from the laptop, and place it in its case.		2152
5.8	CA performs the following steps to prepare the OS media bundle for storage: A) IW gives the new OS media bundle TEB to the CA, then using the information below, verifies it matches while the CA reads the TEB number aloud. B) Place 2 HSMFDs and 2 OS media microSD cards into a plastic case. C) Place the plastic case containing 2 HSMFDs and 2 OS media microSD cards along with 1 sheet of paper with the HSMFD hash printout 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-2.0.1) + HSMFD: TEB # BB02638205**		2156
5.9	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).		2157

Place Laptop6E into a TEB

Step	Activity	Initials	Time
5.10	CA performs the following steps to prepare the laptop for storage: A) IW gives the laptop's designated new TEB to the CA, then using the information below, verifies it matches while the CA reads the TEB number aloud. B) Using the information below, IW verifies it matches while CA reads aloud the service tag number from the bottom of the laptop. 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. **Laptop6E: TEB # BB97448394 / Service Tag # 90YDBT3**		2159

Trusted Community Representative Declaration

Step	Activity	Initials	Time
5.11	CA confirms that **Trusted Community Representative Declaration** forms are signed by all CO Successors. IW retains all original copies. **Crypto Officer 4 Successor: Lodrina Cherne**		2200

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
5.12	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps: A) IW gives the new **Luna CO and SO** TEB to the CA, then using the information below, verifies it matches while the CA reads the the TEB number and description aloud. B) CA gives the designated plastic credential case to the CO, then they gather their **Luna CO and SO** credentials, place them in the case, and return it to CA. C) CA along with IW inspects the designated plastic credential case to ensure it contains the CO's **Luna CO and SO** credentials. D) CA places the plastic case into the CO's new TEB, then seals it. E) CA gives the sealing strips to IW for post-ceremony inventory. F) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. G) CA initials the TEB with a ballpoint pen. H) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. I) If applicable, repeat steps **A) to H)** for the **Luna Audit and Domain** TEB and iKeys. J) If applicable, repeat steps **A) to H)** for each individual **Keyper SET** TEB(s). K) CO inspects their TEBs, then initials them with a ballpoint pen. L) CO writes the date and time, signs the credential table of the IW's script, then IW initials the entry. M) CO returns to their seat with their TEBs. N) Repeat steps for all the remaining COs on the list. **Crypto Officer 1: George Michaelson** **Luna CO and SO TEB # BB02638204** **Luna Audit and Domain TEB # BB02638203** **Keyper Set #1 TEB # BB02638202** **Crypto Officer 2: Pia Gruvö** **Luna CO and SO TEB # BB02638201** **Luna Audit and Domain TEB # BB02638200** **Keyper Set #1 TEB # BB02638199** **Crypto Officer 3: Ondřej Filip** **Luna CO and SO TEB # BB02638198** **Luna Audit and Domain TEB # BB02638197** **Keyper Set #1 TEB # BB02638196** **Crypto Officer 4 Successor: Lodrina Cherne** **Luna CO and SO TEB # BB02638195** **Luna Audit and Domain TEB # BB02638194** **Keyper Set #1 TEB # BB02638193** **Keyper Set #2 TEB # BB02638192** **Crypto Officer 6: Hugo Salgado** **Luna CO and SO TEB # BB02638191** **Luna Audit and Domain TEB # BB02638190** **Keyper Set #1 TEB # BB02638189** **Crypto Officer 7: Dileepa Lathsara** **Luna CO and SO TEB # BB02638188** **Luna Audit and Domain TEB # BB02638187** **Keyper Set #1 TEB # BB02638186**		2227

TCR	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	Luna CO and SO TEB # **BB02638204** Luna Audit and Domain TEB # **BB02638203** Keyper Set #1 TEB # **BB02638202**	**George Michaelson**		**2025 Nov** —		
CO2	Luna CO and SO TEB # **BB02638201** Luna Audit and Domain TEB # **BB02638200** Keyper Set #1 TEB # **BB02638199**	**Pia Gruvö**		**2025 Nov** —		
CO3	Luna CO and SO TEB # **BB02638198** Luna Audit and Domain TEB # **BB02638197** Keyper Set #1 TEB # **BB02638196**	**Ondřej Filip**		**2025 Nov** —		
CO4	Luna CO and SO TEB # **BB02638195** Luna Audit and Domain TEB # **BB02638194** Keyper Set #1 TEB # **BB02638193** Keyper Set #2 TEB # **BB02638192**	**Lodrina Cherne**		**2025 Nov** —		
CO6	Luna CO and SO TEB # **BB02638191** Luna Audit and Domain TEB # **BB02638190** Keyper Set #1 TEB # **BB02638189**	**Hugo Salgado**		**2025 Nov** —		
CO7	Luna CO and SO TEB # **BB02638188** Luna Audit and Domain TEB # **BB02638187** Keyper Set #1 TEB # **BB02638186**	**Dileepa Lathsara**		**2025 Nov** —		

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

Step	Activity	Initials	Time
5.13	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		2227
5.14	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.**		2229
5.15	SSC1 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.**		2229
5.16	CA performs the following steps to return each piece of equipment to the safe: 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. **Keyper HSM8E: TEB # BB51184259** **Luna HSM9E: TEB # BB02638207** **Luna BHSM3E: TEB # BB02638206** **Laptop6E: TEB # BB97448394** **OS media (release coen-2.0.1) + HSMFD: TEB # BB02638205** **Note: The shelves in the equipment safe can slide in and out for ease of use.**		2231

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
5.17	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.		2232
5.18	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, then ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator adjacent to the Tier 5 (Safe Room) exit door is off.		2232
5.19	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).		2233

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
5.20	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)		2234
5.21	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.**		2235
5.22	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 Return the Credentials to Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
5.23	COs perform the following steps sequentially to return the listed TEBs: A) CO announces their box number, then CA operates the **guard key** in that box's **lower lock** with the key blade facing **downward**. B) CO operates their **tenant key** in that box's **upper lock** with the key blade facing **upward**, then opens the safe deposit box. C) CO reads aloud the TEB number, verifies integrity of TEB, then presents it to the audit camera above. D) CO places their TEB(s) in their safe deposit box, locks it, then removes their key. E) CO writes the date and time, then signs the safe log where **"Return"** is indicated. F) IW verifies the completed safe log entry, then initials it. G) CA locks the safe deposit box, then removes the guard key. **Crypto Officer 1: George Michaelson - Box # 1238** **Luna CO and SO TEB # BB02638204** **Luna Audit and Domain TEB # BB02638203** **Keyper Set #1 TEB # BB02638202** **Crypto Officer 2: Pia Gruvö - Box # 1264** **Luna CO and SO TEB # BB02638201** **Luna Audit and Domain TEB # BB02638200** **Keyper Set #1 TEB # BB02638199** **Crypto Officer 3: Ondřej Filip - Box # 1241** **Luna CO and SO TEB # BB02638198** **Luna Audit and Domain TEB # BB02638197** **Keyper Set #1 TEB # BB02638196** **Crypto Officer 4 Successor: Lodrina Cherne - Box # 1239** (Retrieve keys from lock) **Luna CO and SO TEB # BB02638195** **Luna Audit and Domain TEB # BB02638194** **Keyper Set #1 TEB # BB02638193** **Keyper Set #2 TEB # BB02638192** **Crypto Officer 6: Hugo Salgado - Box # 1242** **Luna CO and SO TEB # BB02638191** **Luna Audit and Domain TEB # BB02638190** **Keyper Set #1 TEB # BB02638189** **Crypto Officer 7: Dileepa Lathsara - Box # 1263** **Luna CO and SO TEB # BB02638188** **Luna Audit and Domain TEB # BB02638187** **Keyper Set #1 TEB # BB02638186** **Note: Arrows on the safe deposit box doors indicate key type and blade direction.**		2240

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
5.24	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry, then initials it.		2249
5.25	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, then ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator adjacent to the Tier 5 (Safe Room) exit door is off.		2249
5.26	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).		2250

Act 6: 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
6.1	CA reads all exceptions that occurred during the ceremony.		2252
6.2	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.**		2256
6.3	CA reviews IW's script, then signs the participants list.		2259
6.4	IW signs the list and records the completion time.		2300

Retiring Crypto Officers

Step	Activity	Initials	Time
6.5	CA acknowledges all retiring Crypto Officers and presents them with a token of our appreciation. **Robert Seastrom**		

Stop Online Streaming and Recording

Step	Activity	Initials	Time
6.6	CA acknowledges the participation of the online participants, then instructs the SA to stop the online streaming.		
6.7	CA instructs the SA to stop the audit camera video recording.		
6.8	CA informs onsite participants of post ceremony activities.		
6.9	Ceremony participants take a group photo.		
6.10	Ceremony participants gather their personal items, ensure their area is free of trash/debris, and move to Tier 3 to sign out.		

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 hashes for the HSMFD flash drives.

[5] **kskm-keymaster:** An application that creates and deletes keys and performs a key inventory. More information and the keytools source code can be found at https://github.com/iana-org/dnssec-keytools

[6] **kskm-ksrsigner:** An application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK. More information and the keytools source code can be found at https://github.com/iana-org/dnssec-keytools

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

[8] **printlog:** A bash script used to print the Key Signing Log output.

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

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

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

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

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

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.

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.

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

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

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

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.

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

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

SO (Security Officer): Required for administration of the HSMs. These credentials are also used for the Partition Security Officer role.

Audit: Required to access transaction logs from the HSMs.

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: Key Ceremony Script (by IW) on page 56.

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: Access Control System Configuration Review (by SA) on page 57.

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: Firewall Configuration Review (by SA) on page 58. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 59**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

Appendix C: IW Key Ceremony Script Attestation

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

IW: **Patrick Jones**

Signature:

_____

Date: 2025 Nov __

Appendix D: SA Access Control System Configuration Review

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: **20250424 00:00:00 to 20251114 00:00:00 UTC.**

SA:

_____

Signature:

_____

Date: 2025 Nov __

Appendix E: SA Firewall Configuration Review

I have reviewed and confirmed that the firewall configuration satisfies the requirements of the DNSSEC Practice Statement with version 8th Edition (2025-04-14). No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA:

_____

Signature:

_____

Date: 2025 Nov __