Root DNSSEC KSK

Administrative Ceremony 59
Backup HSM Acceptance Testing

Wednesday 12 November 2025

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

This ceremony is executed in accordance to the DNSSEC Practice Statement for the Root Zone KSK Operator 8th Edition (2024-04-14)

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
OP = Operator
PO = Partition Security Officer
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 the time of completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Andres Pavez / PTI		2025 Nov —	
IW	Aaron Foley / PTI			
SSC1	Rob Hoggarth / ICANN			
TCR1	George Michaelson			
TCR2	Pia Gruvö			
TCR4	Rob Seastrom			
TCR6	Hugo Salgado			
TCR7	Dileepa Lathsara			

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 Administrative Ceremony

The Root DNSSEC Key Signing Key (KSK) Administrative Ceremony is a scripted meeting where individuals with specific roles perform tasks related to support the operation of the Root Zone KSK. Administrative Ceremonies include all ceremonies that do not require use of the private key component of the root zone DNSSEC KSK, such as enrollment or replacement of a trusted role, media deposit or extraction, equipment acceptance testing or maintenance, etc. The process is audited by a third party firm for compliance with SOC 3 framework. The script and recordings are published online for the wider Internet community to review.

Ceremony Guidelines:

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

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony

The CA initiates the ceremony by performing the steps below:

- Verify that the audit cameras are recording
- 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

Initiate and Summarize the Ceremony

Step	Activity	Initials	Time
1.1	CA confirms that required audit cameras are recording.		1931
1.2	CA welcomes all participants to Acceptance Testing Ceremony 59 on Wednesday 12 November 2025, and summarizes the purpose of the ceremony.		1932
1.3	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room) log, then performs a roll call using the participants list on page 2.		1934
1.4	CA asks that any first-time ceremony participants in the room introduce themselves.		1934

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
1.5	CA reviews emergency evacuation procedures with onsite participants.		1934
1.6	CA explains the use of personal electronic devices during the ceremony.		1935

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: 2025 11 12 T 1935 **Note: All entries into this script or any logs should follow this common source of time.**		1935

Act 2: Backup HSM (Tier 7) Acceptance Testing

The CA performs the Backup HSM Acceptance Testing by executing the following steps:

- Set up and configure the testing laptop, peripherals, and connections
- Inspect the Backup HSM's Tamper Evident Bag for tamper evidence
- Power on Backup HSM
- Recover Backup HSM from Secure Transport Mode (STM)
- Import acceptance testing credentials
- Configure Backup HSM Policies
- Initialize Backup HSM
- Factory Reset / zeroize / Backup HSM and power off
- Store the Backup HSM inside of a Tamper Evident Bag

Laptop Setup

Step	Activity	Initials	Time
2.1	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.		1936
2.2	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 # 1** 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 HDMI cable for the external HDMI display to port **B1** on the **back** of the laptop. F) Connect the USB-C to USB-B cable for the printer to port **R1** on the **right** side of the laptop. G) Open the laptop screen, then press the power button to turn the laptop **ON**.		1940
2.3	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**		1940

OS Media coen-2.0.1 Hash Verification

Step	Activity	Initials	Time
2.4	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.**		1940

2.5	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
			1942

Printer Setup

Step	Activity	Initials	Time
2.6	CA confirms that the printer is switched **ON**.		1942
2.7	Using the **Commands** terminal window, the CA executes the command below to configure the printer and print a test page: `configure-printer`		1942

Date Setup

Step	Activity	Initials	Time
2.8	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 "20251112 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.		1944

Connect the Ceremony Hardware Security Module Flash Drive (HSMFD)

Step	Activity	Initials	Time
2.9	CA connects the **HSMFD** into a USB slot, then performs the steps below: A) Wait for the file system window to appear. B) Close the file system window.		1946

Start the Terminal Session Logging

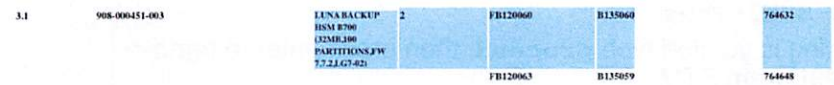
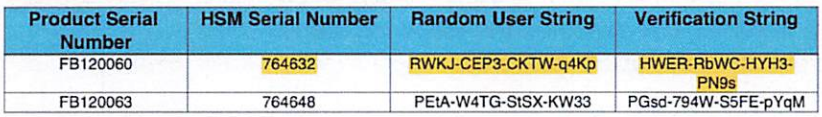
Step	Activity	Initials	Time

2.10	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-20251112.log`
			1946

HSM Log Folder Creation

Step	Activity	Initials	Time
2.11	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`		1947

Verify Luna BHSM3E (Tier 7) Chain of Custody

Step	Activity	Initials	Time
2.12	CA performs the following steps to prepare **Luna BHSM3E**. A) Place **Luna BHSM3E** on the ceremony table leaving it enclosed in its vendor-supplied TEB. B) Inspect the vendor-supplied HSM TEB for tamper evidence. C) Match the HSM serial number and vendor-supplied TEB with the email sent by the vendor (See Appendix A: HSM Chain of Custody - TEB on page 20). If these do not match, re-package HSMs, terminate the ceremony, and return HSMs.  D) Match the Secure Transport Mode (STM) Random User and Verification strings with the email sent by the vendor (See Appendix B: HSM Chain of Custody - STM on page 21).  E) Remove and discard the TEB, antistatic bag, and protective display film, then place **Luna BHSM3E** on its designated stand face down to allow the audit camera to record its serial number. F) Flip **Luna BHSM3E** over face up in its designated stand, then affix the pre-printed label below the display on the lower bezel. **Luna BHSM3E:** **TEB # B135060 / Serial # 764632** **STM Random User String:** `RWKJ-CEP3-CKTW-q4Kp` **STM Verification String:** `HWER-RbWC-HYH3-PN9s`		1952 2010

Product Serial Number	HSM Serial Number	Random User String	Verification String
FB120060	764632	RWKJ-CEP3-CKTW-q4Kp	HWER-RbWC-HYH3-PN9s
FB120063	764648	PEtA-W4TG-StSX-KW33	PGsd-794W-S5FE-pYqM

Power ON Luna BHSM3E (Tier 7)

Step	Activity	Initials	Time
2.13	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**		1954 2015

764648

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

Step	Activity	Initials	Time

2.14	Using the **Commands** terminal window, the CA executes the following steps to recover the HSM from STM:
	A) Launch the **LunaCM** application:
	`lunacm`
	B) Recover **Luna BHSM3E** from STM:
	`stm recover -randomuserstring RWKJ-CEP3-CKTW-q4Kp`
	Note: This will take approximately 3 minutes to process. The result is required to proceed to the next step.
	C) Confirm the verification string matches:
	`HWER-RbWC-HYH3-PN9s`
	D) Once the string is verified type `proceed`, then press enter to remove **Luna BHSM3E** from STM.
			2020

EXCEPTION - BRICK HSM - UI AND USB UNRESPONSIVE 2007 RETURN TO 2.12

Import Audit Credentials

Step	Activity	Initials	Time
2.15	Using the **LunaCM** terminal, CA executes the following steps: A) Initiate the creation of the **audit** credentials: `role init -name au` B) Type `proceed`, then press enter to continue. C) Follow the instructions on the **Luna BHSM3E touchscreen** to register a 2 of 3 **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 2"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue. G) When **Luna BHSM3E** returns to its dashboard, remove the last **audit** iKey. **Note: Use credentials that haven't been used previously during this ceremony when possible. The credentials being used in this ceremony are designated for acceptance testing only and do not contain production materials. For a summary of credential roles and their purpose see Appendix C: Glossary number [13] and [14] on page 22.**		2022 2020

Configure Luna BHSM3E (Tier 7) Audit Settings

Step	Activity	Initials	Time

2.16	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 2"** is displayed, remove the previous iKey and insert a different randomly selected **audit** iKey, then press continue.
	E) When **Luna BHSM3E** returns to its dashboard, remove the last **audit** iKey.
	F) Using the **LunaCM** terminal, synchronize the HSM's clock with the host time:
	`audit time sync`
	G) Set the filepath where log files are written:
	`audit config path /media/HSMFD/BHSM3E`
	H) Set audit logging configuration:
	`audit config evmask all,failure,success`
	I) Type `proceed`, then press enter to continue.
	J) Set audit logging rotation interval:
	`audit config interval hourly@00`
	K) Set audit logging maximum log file size:
	`audit config size 4096k`
	L) Show the audit logging configuration:
	`audit config get`
	M) 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`
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. The credentials being used in this ceremony are designated for acceptance testing only and do not contain production materials. For a summary of credential roles and their purpose see Appendix C: Glossary number [13] and [14] on page 22.
			2025

Initialize the Luna BHSM3E (Tier 7) Administrative Partition

Step	Activity	Initials	Time
2.17	Using the **LunaCM** terminal, CA executes the following steps: **Note: The CA may delegate narration of this step to the 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 2 of 3 **SO** and **domain** credential set: **Note: If the Luna BHSM3E touchscreen is off, tap it once to activate the display.** D) When **"Register your Security Officer..."** is displayed, select **"Use existing quorum of iKeys"**, then press continue. E) When **"Please insert first iKey"** is displayed, insert a randomly selected **SO** iKey, then press continue. F) When **"Please insert iKey 2 of 2"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue to automatically initiate **SO** authentication. G) When **"Please ensure an iKey is inserted"** is displayed, leave the current iKey inserted, then press continue. H) When **"Please insert iKey 2 of 2"** is displayed, remove the previous iKey, insert a different randomly selected **SO** iKey, then press continue to initiate **domain** registration. I) When **"Set up your domain..."** is displayed, remove the last iKey, select **"Join existing domain"**, then press continue. J) When **"Please insert first iKey"** is displayed, insert a randomly selected **domain** iKey, then press continue. K) When "**Please insert iKey 2 of 2"** is displayed, remove the previous iKey and insert a different randomly selected **domain** iKey, then press continue. L) When **Luna BHSM3E** returns to its dashboard, remove the last **domain** iKey. **Note: Use credentials that haven't been used previously during this ceremony when possible. The credentials being used in this ceremony are designated for acceptance testing only and do not contain production materials. For a summary of credential roles and their purpose see Appendix C: Glossary number [13] and [14] on page 22.**		1028

Configure Luna BHSM3E (Tier 7) Global Policies

Step	Activity	Initials	Time

2.18	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~~` 103 - EXCEPTION
	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 2"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue.
	G) When **Luna BHSM3E** returns to its dashboard, remove the last **SO** iKey.
	H) Using the **LunaCM** terminal, activate FIPS mode:
	`hsm changehsmpolicy -policy 55 -value 1`
	I) Verify **Luna BHSM3E** is in FIPS approved operation mode:
	`hsm showinfo`
	
	Note: Use credentials that haven't been used previously during this ceremony when possible. The credentials being used in this ceremony are designated for acceptance testing only and do not contain production materials. For a summary of credential roles and their purpose see Appendix C: Glossary number [13] and [14] on page 22.
			2032

Erase / Zeroize / Factory Reset Luna BHSM3E (Tier 7)

Step	Activity	Initials	Time

2.19	Using the **LunaCM** terminal, CA executes the following steps to factory reset **Luna BHSM3E**:
	A) Verify the admin partition slot number:
	`slot list`
	B) Select the **Luna BHSM3E** admin partition slot:
	`slot set -s ~~105~~` 103
	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 2"** is displayed, remove the previous iKey and insert a different randomly selected **SO** iKey, then press continue.
	G) When **Luna BHSM3E** returns to its dashboard, remove the last **SO** iKey.
	H) Using the **LunaCM** terminal, reset **Luna BHSM3E** to factory settings:
	`hsm factoryreset`
	I) Type `proceed`, then press enter to continue.
	J) Verify the **Luna BHSM3E** dashboard indicates the **HSM is not initialized**.
			2034

Place Luna BHSM3E (Tier 7) into Secure Transport Mode (STM)

Step	Activity	Initials	Time

2.20	CA executes the following steps:
	A) Verify the admin partition slot number:
	`slot list`
	B) Select the **Luna BHSM3E: Serial # 764632** admin partition slot:
	`slot set -s 105` 103
	C) Place **Luna BHSM3E** into STM:
	`stm transport`
	D) Type `proceed`, then press enter to continue.
	E) Verify the **Luna BHSM3E** dashboard indicates the device is in **Secure Transport Mode** and the random and verification strings are displayed in the terminal window.
			2037

Print Luna BHSM3E Secure Transport Mode (STM) Strings

Step	Activity	Initials	Time

2.21	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 "BHSM3E AT59" && 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 BHSM3E 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**
			2039

Place Luna BHSM3E (Tier 7) in the TEB

Step	Activity	Initials	Time
2.22	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 and 1 sheet of paper with the printed STM strings 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 TEB on the cart. **Luna BHSM3E: TEB # BB02638210 / Serial # 764632**		2042

764648

Act 3: Secure Hardware

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

- Store Acceptance Testing Credentials in Plastic Cases
- Copy the Hardware Security Module Flash Drive (HSMFD) contents
- Print log information
- Along with IW, escort SSC1 and equipment cart into Tier 5 (Safe Room) to place equipment to Safe #1

Store Acceptance Testing Credentials in Plastic Cases

Step	Activity	Initials	Time
3.1	CA places the **SO, CO, domain, and audit** credentials into plastic cases and hands them to RKOS for use in future acceptance testing ceremonies.		2043

Stop logging the Terminal Session

Step	Activity	Initials	Time
3.2	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.** B) Disconnect the USB HSM cables from the laptop.		2044

Print Logging Information

Step	Activity	Initials	Time
3.3	CA executes the following commands to print a copy of the logging information: A) `print-script script-202511*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**		2044

Prepare Blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
3.4	Using the **Commands** terminal window, the CA executes the command below to display the contents of the HSMFD: `ls -ltrR`		2048
3.5	CA executes the following command to print two copies of the hash for the HSMFD content: `hsmfd-hash -p` **Note: One copy for each audit bundle.**		2049
3.6	CA executes the command below and follows the interactive prompts in the terminal window to create **one** HSMFD copy. 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.**		2052

EXCEPTION- CA WENT INTO /TMP BEFORE 3.6 HILARITY ENSUED
RECOVERED BY GOING INTO /MEDIA/HSMFD AND RESTARTING 3.6

Power OFF the Laptop

Step	Activity	Initials	Time
3.7	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.**		2054
3.8	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.		2055

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
3.9	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
3.10	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.**		2102
3.11	Perform the following steps to update the safe log: A) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. B) IW provides the pre-printed safe log to SSC1. C) SSC1 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. D) IW verifies this entry then initials it.		2104
3.12	CA performs the following steps to place the HSM into the Safe: A) CAREFULLY remove the equipment TEB from the cart. B) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 (Equipment Safe). C) Write the date, time, and signature on the safe log where **"Place"** is indicated. D) IW verifies the safe log entry, then initials it. **Luna BHSM3E: TEB # BB02638210 / Serial # 764632**		2106 ~~2056~~

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
3.13	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.		2106
3.14	SSC1 returns the safe log to Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). 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.		2107
3.15	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		2107

Act 4: Close the Administrative Ceremony

The CA will finish the ceremony by:

- Reading all exceptions that occurred during the ceremony
- Calling the ceremony participants to sign the IW's script
- Stopping the video recording
- Ensuring that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Preparing the audit bundle materials

Participants Sign IW's Script

Step	Activity	Initials	Time
4.1	CA reads all exceptions that occurred during the ceremony.		2110
4.2	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.**		2112
4.3	CA reviews IW's script, then signs the participants list.		2113
4.4	IW signs the list and records the completion time.		2114

Stop Recording

Step	Activity	Initials	Time
4.5	CA stops the audit camera video recording.		2115
4.6	Ceremony participants gather their personal items, ensure their area is free of trash/debris, and move to Tier 3 to sign out.		2115

Appendix A: HSM Chain of Custody - TEB

The following document contains the HSM(s) serial number and TEB(s) number dispatched from the vendor.

THALES

Shipment Confirmation

Greetings from Thales,

Thank you for your recent order 10463434. We are pleased to inform you that one or more of your items has shipped. Please see the details of the shipment below. If you ordered more than one item, the others may ship separately and you will receive additional notifications.

- The Thales Team.

Ship To: ICANN - INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
Andres Pavez
12025 WATERFRONT DRIVE SUITE 300
LOS ANGELES - CA
United States - 90094
Phone: -4105995192

Order Number : 10463434
Customer PO : 37807929
Delivery Num. : 7500845
Total Boxes : 4
Actual Ship Date : 12-Jun-2025
Carrier Name : FEDEX
Shipment Method : FEDEX-Parcel-Ground
*** Tracking Num. :** 434587096207 [fedex.com]

* 1. Tracking number may not be recognized in the carrier's system until a slightly later time.
2. When the tracking number indicates 'Phantom Ship', it means this Shipment Confirmation is a duplicate of one(s) previously sent and is not related to a new shipment.

Items In Your Shipment

Line Num	Item Number	Description	Quantity Shipped	<---------- Serial Numbers ----------> Product	Tamper Bag	Tamper Seal	HSM
1.1	908-000451-003	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)	1	FB120062	B135061		764635
2.1	909-000004-002	IKEY 1000 10-PACK,LUNA REMOTE PED;STM & AUDIT KEYS,PI,USB,ROHS	3	R240425001	B140980		
				R240425003	B140982		
				R240425023	B141002		
3.1	908-000451-003	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)	2	FB120060	B135060		764632
				FB120063	B135059		764648
4.1	908-000450-001	LUNA USB HSM U700 (32MB,1 PARTITION,FW 7.7.2,LG7-02)	1	FB120064	B135063		764639

Appendix B: HSM Chain of Custody - STM

The following document contains the HSM(s) STM information dispatched from the vendor.

THALES

Thales Luna HSM Secure Transport Mode

Thank you for your recent Thales Luna HSM order. Please find below the information required to validate the integrity of the Luna HSM firmware. This provides the assurance that the Luna HSM has not been tampered with or modified during transport.

Please refer to the "Secure Transport Mode" chapter of the Administration guide for detailed steps.

Sold To Customer:	TD SYNNEX CORPORATION		
End Customer:	ICANN - INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS		
Customer Purchase Order:	37807929	**Thales Sales Order:**	10463434
Item Number:	908-000451-003	**Quantity:**	2
Description:	LUNA BACKUP HSM B700 (32MB,100 PARTITIONS,FW 7.7.2,LG7-02)		
Order Book Date:	06/06/2025		

Product Serial Number	HSM Serial Number	Random User String	Verification String
FB120060	764632	RWKJ-CEP3-CKTW-q4Kp	HWER-RbWC-HYH3-PN9s
FB120063	764648	PEtA-W4TG-StSX-KW33	PGsd-794W-S5FE-pYqM

Appendix C: 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 D: Audit Bundle Checklist

1. Administrative Ceremony Script (by IW)

Hard copies of the IW's administrative ceremony script, including notes and attestation. See Appendix E: Administrative Ceremony Script (by IW) on page 24.

2. Audio-Visual Recordings from the Administrative Ceremony (by CA)

One set of the audit camera footages.

3. 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 E: Administrative Ceremony Script (by IW)

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

IW:

_____

Signature:

_____

Date: 2025 Nov __