Root DNSSEC KSK Ceremony 53-1

Thursday 25 April 2024

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

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

Abbreviations

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

Participants

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

Title / Roles	Printed Name	Signature	Date	Time
CA	David Huberman / ICANN		2024 Apr —	
IW	Andy Newton / ICANN			
SSC1	Fernanda Iunes / ICANN			
SSC2	Hope Shafer / ICANN			
CO1	Frederico Neves			
CO2	Pia Gruvö			
CO3	Ondrej Filip			
CO4	Robert Seastrom			
CO5	Nomsa Mwayenga			
CO6	Hugo Salgado			
CO7	Dileepa Lathsara			
RKSH1	Sebastian Castro			
RKSH2	Ondřej Surý			
RKSH3	Kristian Ørmen			
RKSH4	Jiankang Yao			
RKSH5	Bevil Wooding			
RKSH6	John Curran			
RKSH7	Dave Lawrence			
RZM	Trevor Davis / Verisign			
AUD	Melanie Chen / RSM			
AUD	Grant An / RSM			
SA	Darren Kara / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			

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

Instructions for a Root DNSSEC KSK Ceremony

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

Ceremony Guidelines:

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

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

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

The CA and IW will then escort the 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

Sign into Tier 4 (Key Ceremony Room)

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

Emergency Evacuation Procedures and Electronics Policy

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

Verify the Time and Date

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

Open Safe #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.)		
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.**		
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 pre-printed safe log 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.		

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, and removes their key. 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. **CO1: Frederico Neves - Box # 1239** **Set # 1 TEB # BB02638669** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02638534** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO2: Pia Gruvö - Box # 1264** **Set # 1 TEB # BB02638668** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02639498** (Retain) Last Verified: KSK Ceremony 47 2022-11-03 **CO3: Ondrej Filip - Box # 1241** **Set # 1 TEB # BB02639557** (Check and Return) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02638533** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO4: Robert Seastrom - Box # 1243** **Set # 1 TEB # BB02638667** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02639551** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO5: Nomsa Mwayenga - Box # 1262** **Set # 1 TEB # BB02638666** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02638665** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **CO6: Hugo Salgado - Box # 1242** **Set # 1 TEB # BB02638664** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02638530** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO7: Dileepa Lathsara - Box # 1263** **Set # 1 TEB # BB02639495** (Check and Return) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02638529** (Retain) Last Verified: KSK Ceremony 49 2023-04-27 **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.**		

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.		
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.		
1.14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).		

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.)		
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.**		
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 pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies the entry, then initials it.		

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

Step	Activity	Initials	Time
1.18	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. **HSM5E: TEB # BB51184250 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **HSM6E: TEB # BB51184243 (Stored for Backup Purposes)** Last Verified: KSK Ceremony 49 2023-04-27 **HSM7E: TEB # BB51184251 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **HSM8E: TEB # BB51184252 (Check and Return)** Last Verified: KSK Ceremony 51 2023-11-30 **Laptop3: TEB # BB97448418 (Place on Cart)** Last Verified: KSK Ceremony 49 2023-04-27 **Laptop4: TEB # BB81420078 (Check and Return)** Last Verified: KSK Ceremony 51 2023-11-30 **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **KSK-2017: TEB # BB02638662 (Check and Return)** Last Verified: KSK Ceremony 51 2023-11-30 **KSK-2023: TEB # BB02638661 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.** **The shelves in the equipment safe can slide in and out for ease of use.**		

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

Act 2: Introduce New OS Media

The CA will introduce new OS media by performing the following steps:

- Verify the new OS media matches the checksum published online at https://github.com/iana-org/coen
- Calculate new OS media checksums using the current OS media. Once the new OS media hash has been verified it will be ready to use in production
- Discard previous OS media after new OS media has been verified

Laptop3 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 on the ceremony table. b) Inspect the equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **Laptop3: TEB # BB97448418 / Service Tag # J8SVSG2** Last Verified: KSK Ceremony 49 2023-04-27 **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663** Last Verified: KSK Ceremony 51 2023-11-30 **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.**		
2.2	CA performs the following steps to confirm that no hard drive and battery are in the laptop: a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty.		
2.3	CA ensures the **lock switch** on the left side of the listed SD card is slid down to the lock position: **OS media release coen-1.0.0** **Copy # 1**		
2.4	CA performs the following steps to boot the laptop: a) Connect the external HDMI display cable. b) Connect the power supply. c) Insert the **OS media release coen-1.0.0 Copy # 1**. d) Switch it ON.		
2.5	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**		

OS Media coen-1.0.0 Checksum Verification

Step	Activity	Initials	Time

2.6	Using the **Commands** terminal window, CA executes the following steps:
	a) Verify the byte count of the SD card matches the **OS media release coen-1.0.0** ISO size **375431168** by running the following command:
	`df -B1 /dev/sda`
	b) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sda | sha2wordlist`
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	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:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1		

OS Media coen-1.1.0 Acceptance Test

Step	Activity	Initials	Time
2.7	CA connects the external SD card reader to a USB port in the laptop.		
2.8	CA ensures the **lock switch** on the left side of the SD card is slid down to the lock position.		
2.9	CA inserts the new **OS media release coen-1.1.0** SD card into the external SD card reader, then using the **Commands** terminal window performs the following steps: **Note: The SD card should be inserted upside-down with the writing on top of the SD card reader visible.** a) Confirm the external SD card ID of **`/dev/sdb`** by executing: **`lsblk`** b) Mount the external SD card by executing: **`mount /dev/sdb /mnt`** c) Verify the byte count of the SD card matches the **OS media release coen-1.1.0** ISO size **602406912** by running the following command: **`df -B1 /dev/sdb`** d) Calculate the SHA-256 hash by executing: **`head -c 602406912 /dev/sdb | sha2wordlist`** e) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.** f) Unmount the external SD card by executing: **`umount /dev/sdb`** SHA-256 hash: **2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8** PGP Words: **blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous** **Note: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1**		
2.10	CA removes the new OS media SD card, then places it on the ceremony table. **Note: The tested OS media must be placed on the ceremony table where it is visible to the audit camera and the participants**		
2.11	CA repeats steps **2.8** to **2.10** for the 2nd copy of the new **OS media release coen-1.1.0** SD card.		
2.12	CA disconnects the external SD card reader from the laptop.		

Retire Previous OS Media coen-1.0.0

Step	Activity	Initials	Time
2.13	CA performs the following steps to switch OFF the laptop and remove the OS media: a) Remove the OS media from the laptop, and place it in its case. b) Power **OFF** the laptop by pressing the power button. c) Disconnect all connections from the laptop. d) Discard all copies of the **OS media release coen-1.0.0**.		

Act 3: Equipment Setup

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

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

Laptop3 Setup

Step	Activity	Initials	Time
3.1	CA performs the following steps to prepare each item listed below: a) Remove the TEB from the cart, then place it on the ceremony table. b) Inspect the equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM7E: TEB # BB51184251 / Serial # H2110009** Last Verified: KSK Ceremony 51 2023-11-30 **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.**		
3.2	CA ensures the **lock switch** on the left side of the listed SD card is slid down to the lock position: **OS media release coen-1.1.0** **Copy # 1**		
3.3	CA performs the following steps to boot the laptop: a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into a USB port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Insert the **OS media release coen-1.1.0 Copy # 1**. f) Switch it ON.		
3.4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**		

OS Media coen-1.1.0 Checksum Verification

Step	Activity	Initials	Time

3.5	Using the **Commands** terminal window, CA executes the following steps:
	a) Verify the byte count of the SD card matches the **OS media release coen-1.1.0** ISO size **602406912** by running the following command:
	`df -B1 /dev/sda`
	b) Calculate the SHA-256 hash by executing:
	`head -c 602406912 /dev/sda | sha2wordlist`
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	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:
	2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8
	PGP Words:
	blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous
	
	Note: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1		

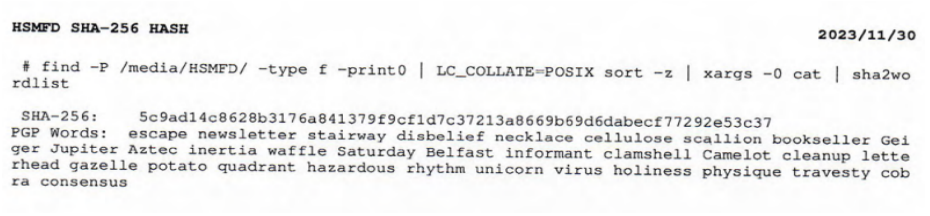
Printer Setup

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

Date Setup

Step	Activity	Initials	Time
3.8	Using the **Commands** terminal window, CA executes the command below to verify the date/time reasonably matches the ceremony clock. `date` If the date/time do not match, perform the following steps: a) Execute `date -s "20240425 HH:MM:SS"` to set the time. **where `HH` is two-digit hour, `MM` is two-digit minutes and `SS` is two-digit seconds.** b) Execute `date` to confirm the date/time matches the clock.		

Connect the Ceremony 51 HSMFD

Step	Activity	Initials	Time
3.9	CA plugs the **Ceremony 51 HSMFD** into a USB slot, then performs the steps below: a) Wait for the file system window to appear. b) Display the HSMFD contents to all participants. c) Close the file system window.		
3.10	Using the **Commands** terminal window, 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.  HSMFD SHA-256 HASH 2023/11/30 # find -P /media/HSMFD/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wordlist SHA-256: 5c9ad14c8628b3176a841379f9cf1d7c37213a8669b69d6dabecf77292e53c37 PGP Words: escape newsletter stairway disbelief necklace cellulose scallion bookseller Geiger Jupiter Aztec inertia waffle Saturday Belfast informant clamshell Camelot cleanup letterhead gazelle potato quadrant hazardous rhythm unicorn virus holiness physique travesty cobra consensus IW confirms that the result matches the SHA-256 hash of the HSMFD using the printed HSMFD hash from the Ceremony 51 OS Media bundle.		

Distribute Unused Ceremony 51 HSMFD

Step	Activity	Initials	Time
3.11	CA gives the unused **Ceremony 51 HSMFD** and the sheet of paper with the printed HSMFD hash to RKOS.		

Start the Terminal Session Logging

Step	Activity	Initials	Time
3.12	Using the **Commands** terminal window, CA executes the command below to change the working directory to HSMFD: **`cd /media/HSMFD`**		
3.13	Using the **Commands** terminal window, CA executes the command below to log activities of the terminal window: **`script script-20240425.log`**		

Start the HSM Output Logging

Step	Activity	Initials	Time
3.14	Using the **HSM Output** terminal window, CA performs the following steps to capture the activity logs of the 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.**		

Power ON HSM7E (Tier 7)

Step	Activity	Initials	Time
3.15	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM7E**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, 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 **H2110009**. e) Scroll down to the end of the terminal window. **HSM7E: Serial # H2110009** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Act 4: Activate HSM7E (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

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
4.1	The CA calls each of the COs listed below sequentially to perform the following steps: a) CO reads aloud the TEB number, then CA inspects it for tamper evidence while the IW verifies its "last verified" information using the specified previous ceremony script. b) CO and CA open the TEB, then the CA removes the credential case to perform the action specified below. **CO2: Pia Gruvö** **Set # 2 TEB # BB02639498** (CO places cards on their designated card holders) Last Verified: KSK Ceremony 47 2022-11-03 **CO4: Robert Seastrom** **Set # 2 TEB # BB02639551** (CO places cards on their designated card holders) Last Verified: KSK Ceremony 45 2022-05-12 **CO7: Dileepa Lathsara** **Set # 2 TEB # BB02638529** (CO places cards on their designated card holders) Last Verified: KSK Ceremony 49 2023-04-27 **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.**		

Enable/Activate HSM7E (Tier 7)

Step	Activity	Initials	Time
	CA performs the following steps to activate the HSM: 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.		
4.2	Confirm the **"READY"** LED on the **HSM** is **ON.** IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ 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 number [14] and [15] on page 41.**		

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
4.3	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		

4.4	CA performs the following steps to test the network connectivity between laptop and HSM:
	a) Select the **Commands** terminal window
	b) Test connectivity by executing:
	`ping hsm`
	c) Wait for responses, then exit by pressing:
	`Ctrl + C`		

Insert the KSRFD

Step	Activity	Initials	Time
4.5	CA plugs the **KSRFD** into an available USB port, 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 1 KSR.**		

Execute the KSR Signer for KSR 2024 Q3

Step	Activity	Initials	Time
4.6	Using the **Commands** terminal window, the CA executes the command below to change the working directory: `cd /media/KSRFD/KSK53-1/`		
4.7	Using the **Commands** terminal window, the CA executes the command below to sign the KSR file: `kskm-ksrsigner`		

Verify the KSR Hash for KSR 2024 Q3

Step	Activity	Initials	Time
4.8	When the hash of the KSR is displayed in the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification **off camera** for the purpose of authentication while maintaining privacy. **Note: If the RZM representative is not physically present in the room, write the representative's name and *"Remote Participant"* next to the name on the signature line.** b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line: **Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS in advance to be included in the final annotated script and audit bundle.** _____ c) The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.		
4.9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		
4.10	CA enters **Yes** in response to **`"Sign KSR?"`** to complete the KSR signing operation. The SKR is located at: **`/media/KSRFD/KSK53-1/skr-root-2024-q3-0.xml`**		

Print Copies of the KSR Signer Log(s)

Step	Activity	Initials	Time
4.11	Using the **Commands** terminal window, the CA executes the commands below to print the KSR Signer log: a) **`printlog kskm-ksrsigner-202404*.log X`** **Note: Replace "X" with the quantity of copies needed for the participants.**		
4.12	IW attaches a copy of the required ksr signer log to their script.		
4.13	Using the **Commands** terminal window, the CA executes the command below to change the working directory: **`cd /media/HSMFD`**		

Copy the Newly Generated SKR(s)

Step	Activity	Initials	Time

4.14	CA executes the following commands using the terminal window:
	a) List the contents of the KSRFD by executing:
	`ls -ltrR /media/KSRFD`
	b) Copy the contents of the KSRFD to the HSMFD by executing:
	`cp -pR /media/KSRFD/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD by executing:
	`ls -ltrR`
	d) Verify it has been copied successfully by executing:
	`diff -qr /media/HSMFD/KSK53-1/ /media/KSRFD/KSK53-1/`
	e) Unmount the KSRFD by executing:
	`umount /media/KSRFD`
	Note: When executing a diff command, a return of no output indicates a match.		

4.15	CA removes the **KSRFD** containing the SKR files, then gives it to the RZM representative. **Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.**		

Disable/Deactivate HSM7E (Tier 7)

Step	Activity	Initials	Time
4.16	CA deactivates the HSM by performing the following steps: **Note: CA will use OP cards not previously utilized in this ceremony if available.** 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. Confirm the **"READY"** LED on the **HSM** is **OFF.** IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ 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 number [14] and [15] on page 41.**		

Place HSM7E (Tier 7) into a TEB

Step	Activity	Initials	Time
4.17	CA switches the HSM power **OFF**, then disconnects the power, serial, and ethernet connections. **Note: DO NOT unplug the cable connections on the laptop.**		
4.18	CA performs the following steps to prepare the HSM for storage: a) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. **HSM7E: TEB # BB51184553 / Serial # H2110009**		

OS Media coen-1.1.0 Checksum Verification

Step	Activity	Initials	Time

4.19	Using the **Commands** terminal window, CA executes the following steps:
	a) Verify the byte count of the SD card matches the **OS media release coen-1.1.0** ISO size **602406912** by running the following command:
	`df -B1 /dev/sda`
	b) Calculate the SHA-256 hash by executing:
	`head -c 602406912 /dev/sda | sha2wordlist`
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	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:
	2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8
	PGP Words:
	blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous
	
	Note 1: The SHA-256 hash of the OS media is being calculated a second time to ensure the contents of the SD card have not been modified during the previous steps.
	Note 2: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1		

Ceremony Break

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

Act 5: Test and Replace Recovery Key Share Holders' (RKSHs) Storage Master Key (SMK) Cards

The currently-issued Recovery Key Share Holders' Storage Master Key Cards were generated in 2010, and should be tested for functionality, then replaced due to age. This will be achieved by performing the following steps:

- Generate a new temporary SMK on the HSM
- Attempt to import an APP key backup encrypted with the production SMK (with an expected failed result). This will demonstrate incompatibility between the temporary SMK and the APP key backup
- Import the production SMK to the HSM using the 2010-era RKSH SMK Cards and successfully import the APP key backup. This will demonstrate compatibility between the production SMK and APP key Backup as well as functionality of the 2010-era RKSH SMK cards
- Generate replacement RKSH SMK cards to replace the existing cards due to age
- Destroy the 2010-era RKSH SMK cards

Note: For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.

HSM5E (Tier 7) Setup

Step	Activity	Initials	Time
5.1	CA performs the following steps to prepare the HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM5E: TEB # BB51184250 / Serial # H1903018** Last Verified: KSK Ceremony 51 2023-11-30 **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.**		

Power ON HSM5E (Tier 7)

Step	Activity	Initials	Time
5.2	CA selects the **HSM Output** terminal window.		
5.3	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM5E**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, 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 **H1903018**. e) Scroll down to the end of the terminal window. **HSM5E: Serial # H1903018** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Recovery Key Share Holders' (RKSHs) Credentials Verification

Step	Activity	Initials	Time
5.4	The CA calls each of the RKSHs listed below sequentially to perform the following steps: a) RKSH reads aloud the TEB number, then CA inspects it for tamper evidence while the IW verifies its "last verified" information using the specified previous ceremony script. b) RKSH and CA open the TEB, then the CA removes the contents to perform the action specified below. **RKSH2: Ondřej Surý** **TEB # A14377098** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH3: Kristian Ørmen** **TEB # BB46592121** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 31 2017-10-18 **RKSH4: Jiankang Yao** **TEB # A14377104** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH5: Bevil Wooding** **TEB # A14377106** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH6: John Curran** **TEB # A14377108** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH7: Dave Lawrence** **TEB # BB91951260** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **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.**		

APP Key Backups

Step	Activity	Initials	Time
5.5	CA performs the following steps to prepare the APP key backups: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Open and discard the TEB, and if not already present, place a corresponding label on the APP key Backup plastic case. e) Remove the APP key cards and place them on the card holder, ensuring their respective backup HSMFDs remain in their plastic case. f) Place the plastic case along with its corresponding sheet of paper with the printed HSMFD hash on its designated area of the ceremony table. **KSK-2023: TEB # BB02638661** Last Verified: KSK Ceremony 51 2023-11-30 **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.**		

Delete the Specified KSK from the HSM

Step	Activity	Initials	Time
5.6	CA performs the following steps to list the KSK(s) present in the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert a randomly selected CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps **c)** to **e)** for the 2nd and 3rd CO cards. g) Select **"2.Key Details"**, press **ENT** to confirm. h) When **"List Keys?"** is displayed, press **ENT**. i) Select **"1.Key Summary"**, press **ENT** to confirm. j) When **"Key Summary?"** is displayed, press **ENT**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st CO card ____ of 7 2nd CO card ____ of 7 3rd CO card ____ 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 number [14] and [15] on page 41.**		
5.7	CA matches the displayed KSK label(s) in the **HSM Output** terminal window. **KSK-2017: Klajeyz** **KSK-2023: Kmrfl3b**		
5.8	CA performs the following steps to delete the specified KSK(s) from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"7.Erase App Keys"**, press **ENT** to confirm. d) When **"Erase App Keys?"** is displayed, press **ENT** to confirm. e) Select **"2.Specify Key"**, press **ENT** to confirm. f) Select the **Kmrfl3b** key by pressing > to move it to the top of the HSM's display, then press **"A"** to select **Kmrfl3b**, then press < to see the key list. **Verify the (*) asterisk is next to Kmrfl3b** then press **ENT** to confirm. **There is no system confirmation prompt**. g) When **Done** is displayed, press **ENT** to return to the App Keys Menu. h) Press **CLR** to return to the Key Mgmt menu.		
5.9	CA performs the following steps to list the KSK from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. CA confirms that the **KSK-2023: Kmrfl3b** has been deleted		

Generate a Temporary SMK

Step	Activity	Initials	Time
5.10	CA performs the following steps to generate a temporary SMK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"1.Generate SMK"**, press **ENT** to confirm. d) When **"Generate SMK?"** is displayed, press **ENT** to confirm. e) When **"SMK Generated"** is displayed, press **ENT** to confirm. f) Press **CLR** once to return to the menu **"Key Mgmt"**.		

Attempt to Import the APP Key Backup (Anticipating a Failed Result)

Step	Activity	Initials	Time
5.11	CA performs the following steps to attempt to import the specified key to demonstrate incompatibility between the temporary SMK and the APP key backup: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required APP key card. g) When **"Remove Card?"** is displayed, remove the APP key card. h) When **"SMK Mismatch"** is displayed, press **ENT** to confirm. i) When **"Restore failed Error code 120D"** is displayed, press **ENT** to confirm. j) Press **CLR** once to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. **KSK-2023: Kmrfl3b** APP Key card # **2** **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 number [14] and [15] on page 41.**		
5.12	CA performs the following steps to list the KSK from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. CA confirms that the **KSK-2023: Kmrfl3b** is still not present in the HSM		

Import the Production SMK Using 2010-era RKSH SMK Cards

Step	Activity	Initials	Time
5.13	CA performs the following steps to import the production SMK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"3.Restore SMK"**, press **ENT** to confirm. d) When **"Restore SMK?"** is displayed, press **ENT** to confirm. e) When **"Insert Card SMK #X?"** is displayed, insert a randomly selected RKSH SMK card. f) When **"Remove Card?"** is displayed, remove the RKSH SMK card. g) Repeat steps **e)** to **f)** for the 2nd, 3rd, 4th, and 5th RKSH SMK cards. h) When **"SMK Restored"** is displayed, press **ENT** to confirm. i) Press **CLR** once to return to the menu **"Key Mgmt"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st RKSH SMK card ____ of 7 2nd RKSH SMK card ____ of 7 3rd RKSH SMK card ____ of 7 4th RKSH SMK card ____ of 7 5th RKSH SMK card ____ 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 number [14] and [15] on page 41.**		

Import the APP key Backup (Anticipating a Successful Result)

Step	Activity	Initials	Time
5.14	CA performs the following steps to import the specified key to demonstrate compatibility between the production SMK and the APP key backup: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required APP key card. g) When **"Remove Card?"** is displayed, remove the APP key card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR** once to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. **KSK-2023: Kmrfl3b** APP Key card # **2** **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 number [14] and [15] on page 41.**		

List the KSKs present in the HSM

Step	Activity	Initials	Time
5.15	CA performs the following steps to list the KSK from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**.		
5.16	CA matches the displayed KSK label(s) in the **HSM Output** terminal window. **KSK-2017: Klajeyz** **KSK-2023: Kmrfl3b**		

Remove the 2010-era RKSH SMK Cards from the Card Holder for Pending Destruction

Step	Activity	Initials	Time
5.17	CA performs the following steps to prepare the 2010-era RKSH SMK cards for destruction: a) Gather set 1 of the 2010-era RKSH SMK cards and place them in an available empty plastic case. b) Set the plastic case aside on the ceremony table for pending destruction. c) Gather set 2 of the 2010-era RKSH SMK cards and place them in an available empty plastic case. d) Set the plastic case aside on the ceremony table for pending destruction.		

Generate Two New Sets of RKSH SMK Cards

Step	Activity	Initials	Time
5.18	CA performs the following steps to issue Recovery Key Share Holder (RKSH) Storage Master Key (SMK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"2.Backup SMK"**, press **ENT** to confirm. d) When **"Backup SMK?"** is displayed, press **ENT** to confirm. e) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**. f) When **"Num Req Cards?"** is displayed, enter **"5"**, then press **ENT**. g) When **"Insert Card #X?"** is displayed, insert the required RKSH SMK card. h) When **"Remove Card?"** is displayed, remove the RKSH SMK card. i) Repeat steps **g)** to **h)** until all the SMK cards have been issued. j) When **"Verify Card #X?"** is displayed, insert the required RKSH SMK card. k) When **"Remove Card?"** is displayed, remove the RKSH SMK card. l) Repeat steps **j)** to **k)** until all the RKSH SMK cards have been verified. m) When **"SMK Backed Up"** is displayed, press **ENT** to confirm. n) Repeat steps **c)** to **m)** to create a **2nd SMK card set**. o) Press **CLR** once to return to the menu **"Key Mgmt"**.		

Clear and Destroy 2010-era RKSH SMK Cards

Step	Activity	Initials	Time
5.19	CA performs the following steps to clear the 2010-era RKSH SMK Cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"4.Clear Cards"**, press **ENT** to confirm. d) When **"Clear Cards?"** is displayed, press **ENT** to confirm. e) When **"Insert Card SMK #X?"** is displayed, take the **SMK #X** card, show the **SMK #X** card to the audit camera and then insert the **SMK #X** card into the HSM's card reader. f) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**. g) When **"Clearing Card Are you sure?"** is displayed, press **ENT** to confirm. h) When **"Remove Card?"** is displayed, remove the SMK card. i) Repeat steps **e)** to **h)** skipping **f)** for the remaining cards in this SMK set. j) Repeat steps **c)** to **i)** for the 2nd SMK set. k) Press **CLR twice** to return to the main menu **"Secured"**.		
5.20	CA uses the shredder to destroy the cleared 2010-era RKSH SMK Cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.		

Place HSM5E (Tier 7) into a TEB

Step	Activity	Initials	Time
5.21	CA switches the HSM power **OFF**, then disconnects the power, serial, and ethernet connections. **Note: DO NOT unplug the cable connections on the laptop.**		
5.22	CA performs the following steps to prepare the HSM for storage: a) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. **HSM5E: TEB # BB51184554 / Serial # H1903018**		

Return the APP key backup into a TEB

Step	Activity	Initials	Time
5.23	CA performs the following steps to prepare the APP key backup for storage: a) Ask the IW for the APP key backup's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Place the APP key backup into its plastic case along with the backup HSMFD c) Place the the plastic case and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the APP key backup TEB 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 APP key backup TEB on the cart. **KSK-2023: TEB # BB02639665**		

Place Recovery Key Share Holders' Credentials into TEBs

Step	Activity	Initials	Time
5.24	The CA calls each of the RKSHs listed below sequentially to the ceremony table to perform the following steps: a) CA asks the IW for the RKSH's designated new primary TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. b) CA asks the IW for the RKSH's designated new backup TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. c) CA places the backup TEB inside of the primary TEB in case the primary TEB is compromised in the future. d) CA places the RKSH note inside of the primary TEB, ensuring it's still legible through the bag. e) RKSH removes their credentials from the card holder, then hands them to the CA. f) CA verifies the credentials, then places them into an available plastic case. g) CA places the plastic case into its designated new TEB, then seals it. h) CA gives the IW sealing strips for post-ceremony inventory. i) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. j) CA initials the TEB with a ballpoint pen. k) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. l) CA gives the TEB containing the cards to the RKSH. m) RKSH inspects the TEB, verifies its contents, then initials it with a ballpoint pen. n) RKSH writes the date and time, signs the credential table of the IW's script, then the IW initials the entry. o) RKSH returns to their seat with their TEB. p) Repeat steps for all the remaining RKSHs' credentials on the list. **RKSH1: Sebastian Castro** **Keyper Credential Primary TEB # BB02639664** **Keyper Credential Backup TEB # BB02639663** **RKSH2: Ondřej Surý** **Keyper Credential Primary TEB # BB02639662** **Keyper Credential Backup TEB # BB02639661** **RKSH3: Kristian Ørmen** **Keyper Credential Primary TEB # BB02639660** **Keyper Credential Backup TEB # BB02639659** **RKSH4: Jiankang Yao** **Keyper Credential Primary TEB # BB02639658** **Keyper Credential Backup TEB # BB02639657** **RKSH5: Bevil Wooding** **Keyper Credential Primary TEB # BB02639656** **Keyper Credential Backup TEB # BB02639655** **RKSH6: John Curran** **Keyper Credential Primary TEB # BB02639654** **Keyper Credential Backup TEB # BB02639653** **RKSH7: Dave Lawrence** **Keyper Credential Primary TEB # BB02639652** **Keyper Credential Backup TEB # BB02639651**		

TCR	TEB #	Printed Name	Signature	Date	Time	IW Initials
RKSH1	TEB # **BB02639664**	**Sebastian Castro**		**2024 Apr __**		
RKSH2	TEB # **BB02639662**	**Ondřej Surý**		**2024 Apr __**		
RKSH3	TEB # **BB02639660**	**Kristian Ørmen**		**2024 Apr __**		
RKSH4	TEB # **BB02639658**	**Jiankang Yao**		**2024 Apr __**		
RKSH5	TEB # **BB02639656**	**Bevil Wooding**		**2024 Apr __**		
RKSH6	TEB # **BB02639654**	**John Curran**		**2024 Apr __**		
RKSH7	TEB # **BB02639652**	**Dave Lawrence**		**2024 Apr __**		

Act 6: Secure Hardware

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

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

Stop Logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
6.1	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) 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.** c) Disconnect the null modem and ethernet cables from the laptop.		

Print Logging Information

Step	Activity	Initials	Time
6.2	CA executes the following commands to print a copy of the logging information: a) **`print-script script-202404*.log`** b) **`print-ttyaudit ttyaudit-tty*-202404*.log`** Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**		

Prepare Blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
6.3	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.**		
6.4	CA executes the command below to display the contents of the HSMFD: **`ls -ltrR`**		
6.5	CA executes the command below and follows the interactive prompts in the terminal window to create **five** HSMFDs copies: **`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.**		

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
6.6	Using the **Commands** terminal window, CA executes the commands below to unmount the HSMFD: a) **`cd /tmp`** b) **`umount /media/HSMFD`** CA removes the HSMFD, then places it on the holder. **Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.**		
6.7	CA performs the following steps to shut down the laptop: a) Power **OFF** the laptop by pressing the power button. b) Disconnect all connections from the laptop. c) Remove the OS media from the laptop, and place it in its case. d) Close all laptop latches.		
6.8	CA performs the following steps to prepare the OS media bundle for storage: a) Ask the IW for the OS media bundle's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Place 2 HSMFDs and 2 OS media SD cards into a plastic card case. c) Place the plastic card case containing 2 HSMFDs and 2 OS media SD cards along with 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS media bundle onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the OS media bundle TEB on the cart. **OS Media (release coen-1.1.0) + HSMFD: TEB # BB02639666**		
6.9	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).		

Place Laptop3 into a TEB

Step	Activity	Initials	Time
6.10	CA performs the following steps to prepare the Laptop for storage: a) Ask the IW for the Laptop's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the service tag number from the bottom of the laptop while the IW verifies it matches the information below. c) Place the Laptop into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the Laptop onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the Laptop TEB on the cart. **Laptop3: TEB # BB81420051 / Service Tag # J8SVSG2**		

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
6.11	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps: a) CA asks the IW for the CO's designated new TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. b) CO removes their credentials from the card holder, then hands them to the CA. c) CA verifies the credentials, then places them into an available plastic case. d) CA places the plastic case into its designated new TEB, then seals it. e) CA gives the IW sealing strips 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) CA gives the TEB containing the cards to the CO. j) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. k) CO writes the date and time, signs the credential table of the IW's script, then the IW initials the entry. l) CO returns to their seat with their TEBs. m) Repeat steps for all the remaining COs' credentials on the list. **CO2: Pia Gruvö** **Set # 2 TEB # BB02639669** **CO4: Robert Seastrom** **Set # 2 TEB # BB02639668** **CO7: Dileepa Lathsara** **Set # 2 TEB # BB02639667**		

TCR	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO2	Set # 2 TEB # **BB02639669**	**Pia Gruvö**		**2024 Apr __**		
CO4	Set # 2 TEB # **BB02639668**	**Robert Seastrom**		**2024 Apr __**		
CO7	Set # 2 TEB # **BB02639667**	**Dileepa Lathsara**		**2024 Apr __**		

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

Step	Activity	Initials	Time
6.12	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
6.13	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.**		
6.14	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.**		
6.15	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. **HSM5E: TEB # BB51184554** **HSM7E: TEB # BB51184553** **Laptop3: TEB # BB81420051** **OS media (release coen-1.1.0) + HSMFD: TEB # BB02639666** **KSK-2023: TEB # BB02639665** **Note: The shelves in the equipment safe can slide in and out for ease of use.**		

Close Safe #1 (Tier 6, Equipment Safe)

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

Open Safe #2 (Tier 6, Credentials Safe)

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

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

Step	Activity	Initials	Time
6.22	COs perform the following steps sequentially to return the listed TEBs: a) CO reads aloud the TEB number, verifies integrity of TEB, then presents it to the audit camera above. b) CO announces their box number, then CA operates the guard key in that box's lower lock with the key blade facing downward. c) CO operates their tenant key in that box's upper lock with the key blade facing upward, then opens the safe deposit box. 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. **CO2: Pia Gruvö** **Box # 1264** **Set # 2 TEB # BB02639669** **CO4: Robert Seastrom** **Box # 1243** **Set # 2 TEB # BB02639668** **CO7: Dileepa Lathsara** **Box # 1263** **Set # 2 TEB # BB02639667**		

Close Safe #2 (Tier 6, Credentials Safe)

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

Act 7: 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
7.1	CA reads all exceptions that occurred during the ceremony.		
7.2	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.**		
7.3	CA reviews IW's script, then signs the participants list.		
7.4	IW signs the list and records the completion time.		

Stop Online Streaming and Recording

Step	Activity	Initials	Time
7.5	CA acknowledges the participation of the online participants, then instructs the SA to stop the online streaming.		
7.6	CA instructs the SA to stop the audit camera video recording.		
7.7	CA informs onsite participants of post ceremony activities.		
7.8	Ceremony participants take a group photo.		

Appendix A: Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes generated during the ceremony, and attestation. See Appendix C on page 43.

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

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

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

Two electronic copies of the following:

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

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

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

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

SA's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix D on page 44.

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

SA's attestation and hard copies of the firewall configuration from the review process. See Appendix E on page 45. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 53-1**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

Appendix C: Key Ceremony Script (by IW)

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

IW: **Andy Newton**

Signature: _____

Date: 2024 Apr __

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

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

a) There were NO discrepancies found in the system configurations, assigned authorizations, and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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

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

Range: **20231130 00:00:00 to 20240426 00:00:00 UTC.**

SA: _____

Signature: _____

Date: 2024 Apr __

Appendix E: Firewall Configuration Review (by SA)

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

SA:

_____

Signature:

_____

Date: 2024 Apr __