Root DNSSEC KSK Ceremony 49

Thursday 27 April 2023

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 6th Edition (2020-11-04)

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	**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	**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	Matthew Larson / ICANN			
IW	Patrick Jones / ICANN			
SSC1	Fernanda Iunes / ICANN			
SSC2	Carlos Reyes / ICANN			
CO1	Frederico Neves			
CO3	Ondrej Filip			
CO4	Robert Seastrom			
CO6 Current	Gaurab Upadhaya			
CO6 Successor	Hugo Salgado			
CO7	Dileepa Lathsara			
RZM	Trevor Davis / Verisign			
AUD	John Leonard / RSM		2023 Apr ___	
AUD	Emmanuel Nkereuwem / RSM			
SA	Moises Cirilo / ICANN			
SA	Darren Kara / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Danielle Rutherford / ICANN			
SW	Isabella Reber / ICANN			
EW	Mimi Rauschendorf			
EW	Bob Arasmith			

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 starts filming before the majority of participants enter Tier 4 (Key Ceremony Room)
- 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 HSM 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 enabled
• 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

The CA and IW will then escort the SSCs and COs into Tier 5 (Safe Room) to retrieve the following materials:

• Safe #1: HSM, laptop, OS media, etc
• Safe #2: The COs' cards required to operate the HSM

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.		
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.		
3	CA asks that any first time ceremony participants in the room introduce themselves.		

Emergency Evacuation Procedures and Electronics Policy

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

Verify the Time and Date

Step	Activity	Initials	Time
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
8	CA transports the guard key and flashlight, and with IW escorts SSC2 and the COs into Tier 5 (Safe Room.)		
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.**		
10	Perform the following steps to complete 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
11	COs perform the following steps sequentially to access the listed TEBs: a) After the CA operates the guard key in the bottom lock, CO reads aloud their safe deposit box number then uses their tenant key to operate the top lock. b) CO opens their safe deposit box, verifies its integrity, then removes the TEBs. c) CO reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above. d) CO performs the actions specified below, then locks their safe deposit box. **Note 1: The CO's key will remain inserted in their assigned safe deposit box lock when specified below.** **Note 2: The COs will retrieve their new safe deposit box keys when specified below.** e) CO writes the date and time, then signs the safe log. f) IW verifies the completed safe log entries, then initials them. **CO1: Frederico Neves** **Box # 1239** **Set # 1 TEB # BB02639501** (Check and Return) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02639564** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO3: Ondrej Filip** **Box # 1241** **OP TEB # BB02639569** (Retain) **SO TEB # BB02639558** (Retain) **Set # 1 TEB # BB02639557** (Check and Return) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02639555** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO4: Robert Seastrom** **Box # 1260** (Key shall remain in lock) **New Box # 1243** (Retrieve keys from lock) **OP TEB # BB91951237** (Retain) **SO TEB # BB02639553** (Retain) **Set # 1 TEB # BB02639552** (Transfer to newly assigned safe deposit box) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02639551** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO6 Current: Gaurab Upadhaya** **Box # 1261** (Key shall remain in lock) **OP TEB # BB91951233** (Retain) **SO TEB # BB02639547** (Retain) **Set # 1 TEB # BB02639545** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02639544** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO7: Dileepa Lathsara** **Box # 1263** **Set # 1 TEB # BB02639495** (Check and Return) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02639494** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **Note: "Last verified" indicates the last time a piece of equipment was 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
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.		
13	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and 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 is off.		
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
15	CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.)		
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.**		

17	Perform the following steps to complete 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.		

Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time

18	CA performs the following steps to extract each piece of equipment from the safe:
	    a) CAREFULLY remove each equipment TEB from the safe.
	    b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera.
	    c) Place each equipment TEB on the cart as specified in the list below.
	    d) Write the date and time, then signs the safe log.
	    e) IW verifies the completed safe log entries, then initials it.
	
	HSM5E: TEB # BB51184531 (Place on Cart)
	Last Verified: KSK Ceremony 45 2022-05-12
	HSM6E: TEB # BB51184532 (Place on Cart)
	Last Verified: KSK Ceremony 47 2022-11-03
	
	Laptop3: TEB # BB81420041 (Place on Cart)
	Last Verified: KSK Ceremony 45 2022-05-12
	Laptop4: TEB # BB81420064 (Check and Return)
	Last Verified: KSK Ceremony 47 2022-11-03
	
	OS media (release coen-0.4.0) + HSMFD: TEB # BB02639502 (Place on Cart)
	Last Verified: KSK Ceremony 47 2022-11-03
	
	KSK-2017: TEB # BB46584614 (Check and Return)
	Last Verified: KSK Ceremony 43 2021-10-14
	
	Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.		

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

Step	Activity	Initials	Time
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.		
20	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, and 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 is off.		
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 to perform the ceremony
- Discard previous OS media after new OS media has been verified

Laptop Setup

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the listed equipment: a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each 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 # BB81420041 / Service Tag # J8SVSG2** Last Verified: KSK Ceremony 45 2022-05-12 **OS media (release coen-0.4.0) + HSMFD: TEB # BB02639502** Last Verified: KSK Ceremony 47 2022-11-03 **Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**		
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.		
3	CA performs the following steps to boot the laptop: a) Connect the external HDMI display cable. b) Connect the power supply. c) Immediately insert the **OS media release coen-0.4.0** after the laptop power is switched ON.		
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 Checksum Verification

Step	Activity	Initials	Time
5	CA uses the terminal window to executes the following steps: a) Calculate the SHA-256 hash by executing: `sha2wordlist < /dev/sr0` b) 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: **8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f** PGP Words: **minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document** **Note: The SHA-256 hash of the OS media release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/49**		

OS DVD Acceptance Test

Step	Activity	Initials	Time
6	CA connects the external DVD drive to the USB port of the laptop.		

7	CA inserts the new **OS media release coen-1.0.0** DVD into the external DVD drive, waits for it to be recognized by the OS, then performs the following steps:
	
	a) Close the file system popup window.
	
	CA uses the terminal window to continues with the following steps:
	
	b) Confirm the drive letter by executing:
	`lsblk`
	
	c) Unmount the drive by executing:
	`umount /dev/sr1`
	
	d) Calculate the SHA-256 hash by executing:
	`sha2wordlist < /dev/sr1`
	
	e) Calculate the SHA-256 hash again, ensuring it matches the result from the previous step by executing:
	`head -c 375431168 /dev/sr1
		sha2wordlist`
		
		Note: The second hash check command will be used to verify the SD media in forthcoming steps to provide confidence that the contents of the DVD and SD media are identical.
		
		f) 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.
		
		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/49		

8	CA removes the new OS media DVD by pressing the eject button on the external DVD drive, 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**		
9	CA repeats step 7 to 8 for the 2nd copy of the new **OS media release coen-1.0.0**.		
10	CA disconnects the external DVD drive from the laptop.		

OS SD Card Acceptance Test

Step	Activity	Initials	Time
11	CA ensures the **lock switch** on the left side of the SD card is slid down to the lock position.		
12	CA inserts the new **OS media release coen-1.0.0** SD card into the SD card drive, then performs the following steps using the terminal window: a) Confirm the drive letter by executing: `lsblk` b) Calculate the SHA-256 hash by executing: `head -c 375431168 /dev/sda	sha2wordlist` c) 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.** 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/49**		
13	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**		
14	CA repeats step 11 to 13 for the 2nd copy of the new **OS media release coen-1.0.0** SD card.		

Retire Previous OS Media

Step	Activity	Initials	Time
15	CA performs the following steps to switch OFF the laptop and remove the OS media: a) Remove the OS media from the laptop. b) Turn 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-0.4.0**.		

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)

Laptop Setup

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the listed equipment: 　a) Remove all equipment TEBs from the cart and place them on the ceremony table. 　b) Inspect each 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. **HSM5E: TEB # BB51184531 / Serial # H1903018** Last Verified: KSK Ceremony 45 2022-05-12 **Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**		
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-1.0.0** **Copy # 1**		
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 the serial port of the laptop. 　c) Connect the external HDMI display cable. 　d) Connect the power supply. 　e) Insert the **OS media release coen-1.0.0 Copy # 1**. 　f) Switch it ON.		
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 Checksum Verification

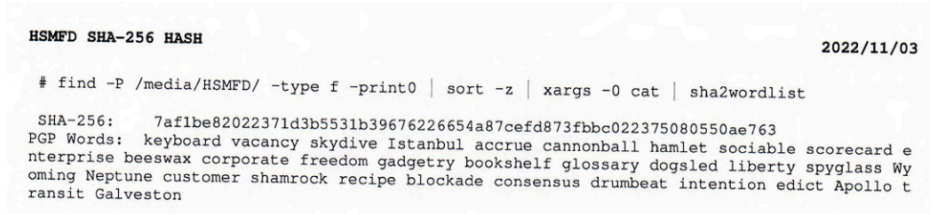| Step	Activity	Initials	Time

5	CA uses the terminal window to executes the following steps:
	    a) Calculate the SHA-256 hash by executing:
	      `head -c 375431168 /dev/sda | sha2wordlist`
	    b) 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/49		

Printer Setup

Step	Activity	Initials	Time
6	CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page: `configure-printer`		

Date Setup

Step	Activity	Initials	Time

7	CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock.
	
	If the date/time do not match, perform the following steps:
	    a) Execute `date -s "20230427 HH:MM:00"` to set the time.
	    where HH is two-digit hour, MM is two-digit minutes and 00 is zero seconds.
	    b) Execute `date` to confirm the date/time matches the clock.		

Connect the HSMFD

Step	Activity	Initials	Time

8	CA plugs the **Ceremony 47 HSMFD** into the USB slot, then performs the steps below:
	    a) Wait for the OS to recognize it.
	    b) Display the HSMFD contents to all participants.
	    c) Close the file system window.		

9	CA executes the command below using the terminal window 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 2022/11/03 # find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist SHA-256: 7af1be82022371d3b5531b39676226654a87cefd873fbbc022375080550ae763 PGP Words: keyboard vacancy skydive Istanbul accrue cannonball hamlet sociable scorecard enterprise beeswax corporate freedom gadgetry bookshelf glossary dogsled liberty spyglass Wyoming Neptune customer shamrock recipe blockade consensus drumbeat intention edict Apollo transit Galveston IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 47 annotated script.		

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 47** and the sheet of paper with the printed HSMFD hash to RKOS.		

Start the Terminal Session Logging

Step	Activity	Initials	Time
11	CA executes the command below using the terminal window to change the working directory to HSMFD: `cd /media/HSMFD`		
12	CA executes the command below to log activities of the **Commands** terminal window: `script script-20230427.log`		

Start the HSM Output Logging

Step	Activity	Initials	Time

13	CA performs the following steps using the **HSM Output** terminal window 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/ttyS0 115200`
	    c) Start logging the serial output by executing:
	      `ttyaudit /dev/ttyS0`
	
	Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.		

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	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 logging screen.** d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H1903018**. e) Scroll down to the end of the logging screen. **HSM5E: Serial # H1903018** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Act 4: Activate HSM (Tier 7) and Generate Signatures

Using the ksr signer application the CA takes the Key Signing Requests (KSRs) to generates the Signed Key Responses (SKRs) by performing the steps below.

- The CA activates the HSM using the COs' cards
- 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 use
- The CA then prints the signer log, backs up the newly created SKRs, and deactivates the HSM

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
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 IW verifies the information using the previous ceremony script where it was last used. b) CO and CA open the TEB, then the CA removes the plastic case containing the cards as specified below. **CO1: Frederico Neves** **Set # 2 TEB # BB02639564** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **CO3: Ondrej Filip** **OP TEB # BB02639569** (Place the plastic case on the table for destruction) **SO TEB # BB02639558** (Place the plastic case on the table for destruction) **Set # 2 TEB # BB02639555** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **CO4: Robert Seastrom** **OP TEB # BB91951237** (Place the plastic case on the table for destruction) **SO TEB # BB02639553** (Place the plastic case on the table for destruction) **Set # 2 TEB # BB02639551** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **CO6 Current: Gaurab Upadhaya** **OP TEB # BB91951233** (Place the plastic case on the table for destruction) **SO TEB # BB02639547** (Place the plastic case on the table for destruction) **Set # 1 TEB # BB02639545** (Place the plastic case on the table for transfer to CO successor) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02639544** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **CO7: Dileepa Lathsara** **Set # 2 TEB # BB02639494** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**		

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time

2	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 the 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.
	
	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 the card is unreadable, gently wipe its metal contacts and try again.		

Check the Network Connectivity Between Laptop and HSM

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

4	CA performs the following steps to test the network connectivity between laptop and HSM:
	    a) Use 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
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 2023 Q3

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSRFD/KSK49/ksr-root-2023-q3-0.xml`		
7	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.		

Verify the KSR Hash for KSR 2023 Q3

Step	Activity	Initials	Time
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.		
9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		
10	CA enters **"y"** in response to **"Is this correct (y/N)?"** to complete the KSR signing operation. The SKR is located in: **/media/KSRFD/KSK49/skr-root-2023-q3-0.xml**		

Print Copies of the KSR Signer Log

Step	Activity	Initials	Time
11	CA executes the commands below using the terminal window to print the KSR Signer log: a) **printlog ksrsigner-202304*.log X** **Note: Replace "X" with the amount of copies needed for the participants.**		
12	IW attaches a copy of the required ksr signer log to their script.		

Copy the Newly Created SKR

Step	Activity	Initials	Time

13	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/KSK49/ /media/KSRFD/KSK49/`
	   e) Unmount the KSRFD by executing:
	     `umount /media/KSRFD`		

14	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.**		

OS Media Checksum Verification

Step	Activity	Initials	Time
15	CA uses the terminal window to executes the following steps: a) Calculate the SHA-256 hash by executing: `head -c 375431168 /dev/sda | sha2wordlist` b) 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 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-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/49**		

Act 5: KSK Generation and Backup

KSK generation

The CA will generate and back up a new KSK by performing the steps below:

• Generate a new KSK
• Back up the new KSK

KSK Generation

Step	Activity	Initials	Time

1	CA executes the command below in the terminal window to generate a new KSK:
	`kskm-keymaster --config /media/HSMFD/KSK49/ksrsigner.yaml`
	`keygen --algorithm RSASHA256 --size 2048`		

Print Copies of the KSK Generation Log

Step	Activity	Initials	Time
2	CA executes the commands below using the terminal window to print the KSK generation log: `printlog kskm-keymaster-202304*.log X` **Note: Replace "X" with the amount of copies needed for the participants.**		
3	IW attaches two copies of the required KSK generation log to their script.		

Record Key Label

Step	Activity	Initials	Time
4	IW records the key label: **Root KSK 2023 Label**: _____		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
5	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 the OP card from the card holder. 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 the card is unreadable, gently wipe its metal contacts and try again.**		

List the KSKs from the HSM

Step	Activity	Initials	Time
6	CA performs the following steps to list the App Keys from the HSM: a) CA selects the **HSM Output** terminal window. b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"5.Key Mgmt"**, press **ENT** to confirm. d) When **"Insert CO Card #X?"** is displayed, insert the CO card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the CO card. g) Repeat steps d) to f) for the 2nd and 3rd CO cards. h) Select **"2.Key Details"**, press **ENT** to confirm. i) When **"List Keys?"** is displayed, press **ENT**. j) Select **"1.Key Summary"**, press **ENT** to confirm. k) 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 the card is unreadable, gently wipe its metal contacts and try again.**		
7	CA matches the displayed KSK label in the **HSM Output** terminal window with the key label indicated on step 4.		

Back up the New KSK

Step	Activity	Initials	Time
8	CA performs the following steps to back up the new App Key: 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 **"1.Backup"**, press **ENT** to confirm. d) When **"Backup?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2.Backup to Card"**, press **ENT** to confirm. f) When **"Smartcard"** is displayed, select **"2.Specify Key"**, press **ENT** to confirm. Use the **>** button to scroll down and position the desired key label on the upper line of the HSM display, then press **"A"** to select the key label (indicated by an asterisk). You may press **"D"** to clear the selection and **<** to scroll up if necessary. Select the key label recorded on step 4, press **ENT** to confirm. g) When **"Insert B/U Card?"** is displayed, insert the required card. h) When **"Remove Card?"** is displayed, remove the App card. i) When **"Backup Success"** is displayed, press **ENT** to confirm. j) Repeat steps c) to i) to create a 2nd Backup. k) Repeat steps c) to i) to create a 3rd Backup. l) Repeat steps c) to i) to create a 4th Backup. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
9	CA uses a sharpie marker to write the key label indicated on step 4 on each APP key card.		

Verify KSK Backup

Step	Activity	Initials	Time

10	CA performs the following steps to verify the App Key backups:
	   a) Utilize the HSM's keyboard to scroll through the menu using < >
	   b) Select **"6.Media Contents"** from the current **"3.App Keys"** menu, press **ENT** to confirm.
	   c) When **"Which Media?"** is displayed, select **"2.View Card"**, press **ENT** to confirm.
	   d) When **"Insert Card?"** is displayed, insert insert the required card.
	   e) When the media type and serial number are shown on the display, press **ENT** to continue.
	   f) When the manufacturer is shown on the display, press **ENT** to continue.
	   g) When the product is shown on the display, press **ENT** to continue.
	   h) When the card size is shown on the display, press **ENT** to continue.
	   i) When **"Output Details?"** is displayed, press **ENT** to confirm.
	   j) When **"Remove Card?"** is displayed, remove the App card.
	   k) Verify the key label displayed in the **HSM Output** terminal window matches the key label recorded on step 4.
	   l) When **"Another Card?"** is displayed, press **ENT** to confirm.
	
	   m) Repeat steps d) to l) to verify a 2nd Backup.
	
	   n) Repeat steps d) to l) to verify a 3rd Backup.
	
	   o) Repeat steps d) to l) to verify a 4th Backup.
	
	   p) Press **CLR thrice** to return to the main menu **"Secured"**.
	
	Each card is returned to its designated card holder after use.
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

Act 6: Destroy OP and SO Cards

The Operator (OP) and Security Officer (SO) cards were originally issued in 2010 and have reached the end of their operational period. New OP and SO card sets were previously generated as replacements, and the original cards will now be destroyed.

The CA will destroy the OP and SO cards by performing the steps below:

- Clear the cards using an HSM's designated clear card function
- Slice through the cards' chips then place the cards in the shredder

Clear and Destroy OP and SO Cards

Step	Activity	Initials	Time
1	CA performs the following steps to clear Operator (OP) and Security Officer (SO) cards: a) CA selects the **HSM Output** terminal window. b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"7.Role Mgmt"**, press **ENT** to confirm. d) When **"Insert Card SO #X?"** is displayed, insert the SO card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the SO card. g) Repeat steps d) to f) for the 2nd and 3rd SO card. h) Select **"4.Clear RoleCard"**, press **ENT** to confirm. i) When **"Clear Card?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"9"**, then press **ENT**. k) When **"Insert Card #X?"** is displayed, take the required card, show the card to the audit camera and then insert the card into the HSM's card reader. l) When **"Are you sure?"** is displayed, press **ENT** to confirm. **Note: The message will differ depending of the card type.** m) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. n) When **"Remove Card?"** is displayed, remove the card. o) Repeat steps k) to n) until the specified cards have been cleared. p) Press **CLR** to return to the main menu **"Secured"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st SO card ـــــ of 7 2nd SO card ـــــ of 7 3rd SO card ـــــ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
2	CA uses the shredder to destroy the cleared OP and SO cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.		

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
3	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. **Note: DO NOT unplug the cable connections on the laptop.**		
4	CA places the HSM into its designated new TEB, then seals it.		
5	CA performs the following steps: a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM TEB on the cart. **HSM5E: TEB # BB51184606 / Serial # H1903018**		

Act 7: KSK Import

The CA will import a new KSK by performing the steps below:

· Set up and power on an HSM where the KSK is to be imported
· Use an App key backup smartcard to import a KSK
· List and verify installed KSKs in the HSM
· Repeat previous steps for additional HSMs if necessary

HSM (Tier 7) Setup

Step	Activity	Initials	Time
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. **HSM6E: TEB # BB51184532 / Serial # H2001001** Last Verified: KSK Ceremony 47 2022-11-03 **Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**		

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
2	CA selects the **HSM Output** terminal window.		
3	CA performs the following steps to prepare the HSM: 　a) Verify the label on the HSM reads **HSM6E**. 　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 logging screen.** 　d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H2001001**. 　e) Scroll down to the end of the logging screen. **HSM6E: Serial # H2001001** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Import the KSK

Step	Activity	Initials	Time

4	CA performs the following steps to access the Key Management menu:
	    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 the 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 card.
	
	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 the card is unreadable, gently wipe its metal contacts and try again.		

5	CA performs the following steps to import KSK:
	    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 KSK card.
	    g) When **"Remove Card?"** is displayed, remove the KSK card.
	    h) When **"Restore Complete"** is displayed, press **ENT** to confirm.
	    i) Press **CLR** to return to the menu **"Key Mgmt"**.
	
	CA uses the card listed below. Card is returned to its designated card holder after use.
	App Key card: **Copy # 1**[*]
	
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

6	CA performs the following steps to list the App Keys from the HSM:
	    a) Utilize the HSM's keyboard to scroll through the menu using < >
	    b) Select **"2.Key Details"** from the current **"Key Mgmt"** menu, 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**.
	    f) Press **CLR** to return to the main menu **"Secured"**.		

7	CA verifies the displayed KSK label in the **HSM Output** terminal window matches the imported key label.		

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
8	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. **Note: DO NOT unplug the cable connections on the laptop.**		
9	CA places the HSM into its designated new TEB, then seals it.		

10	CA performs the following steps:
	    a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.
	    b) Confirm with IW that the TEB number and HSM serial number match below.
	    c) Initial the TEB along with IW using a ballpoint pen.
	    d) Give IW the sealing strips for post-ceremony inventory.
	    e) Place the HSM TEB on the cart.
	
	HSM6E: TEB # BB51184243 / Serial # H2001001		

Act 8: Secure Hardware

The CA will secure the ceremony hardware by performing the steps below:

- Copy the HSMFD contents
- Print log information
- Place the equipment and CO 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 COs' cards to Safe #2

Stop Logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
1	CA performs the following steps to stop logging: a) Disconnect the null modem and ethernet cables from the laptop. b) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: i) Press **Ctrl + C** ii) Execute **exit** c) 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.**		

Print Logging Information

Step	Activity	Initials	Time
2	CA executes the following commands to print a copy of the logging information: a) **print-script script-202304*.log** b) **print-ttyaudit ttyaudit-tty*-202304*.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
3	CA executes the following command **twice** to print **four** copies of the hash for the HSMFD content: **hsmfd-hash -p** **Note: One copy for each KSK Backup bundles, one copy for audit bundle, and one copy for HSMFD package.**		
4	CA executes the command below to display the contents of the HSMFD: **ls -ltrR**		
5	CA executes the command below to create **nine** HSMFDs copies: **copy-hsmfd** **Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.**		

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
6	CA executes the following commands using the terminal window 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.**		
7	CA performs the following steps to switch OFF the laptop and remove the OS media: a) Turn OFF the laptop by pressing the power button. b) Disconnect all connections from the laptop. c) Remove the OS media from the laptop.		
8	CA places 2 HSMFDs, 2 OS media SD cards enclosed in their plastic cases, 2 OS media DVDs, and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seals it.		
9	CA performs the following steps to verify the TEB: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS media TEB on the cart. **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638528**		
10	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).		

Place the KSK Backups into a TEB

Step	Activity	Initials	Time
11	CA performs the following steps: a) CA places **KSK Backup Copy # 1**[*] and **KSK Backup Copy # 2**, and 2 HSMFDs in a plastic case. b) CA places the plastic case and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seals it.		
12	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Calls RKOS to proceed to the ceremony table and initial the TEB using a ballpoint pen. f) Give RKOS the TEB. **App Key Backups: TEB # BB02638527**		
13	CA places **KSK Backup Copy # 1** and **KSK Backup Copy # 2**, and 2 HSMFDs enclosed in their plastic cases, and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seals it.		
14	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the TEB on the cart. **KSK-2023: TEB # BB02638526**		

Place the Laptop into a TEB

Step	Activity	Initials	Time
15	CA places the laptop into its designated new TEB, then seals it.		
16	CA performs the following steps: a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and laptop serial number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the laptop TEB on the cart. **Laptop3: TEB # BB97448418 / Service Tag # J8SVSG2**		

Trusted Community Representative Declaration

Step	Activity	Initials	Time
17	CA confirms that **Trusted Community Representative Declaration** forms are signed by all CO Successors. IW retains all original copies. **CO6 Successor: Hugo Salgado**		

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
18	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps: a) CA takes the TEB and plastic case prepared for the CO. b) CO takes their cards from the card holder and places them inside the plastic case. c) CO gives the plastic case containing the cards to the CA. d) CA places the plastic case into its designated new TEB, reads aloud the TEB number and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony inventory. f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. g) CA gives the TEB containing the cards to the CO. h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. i) CO writes the date and time, then signs the table of the IW's script, then the IW initials the entry. j) CO returns to their seat with their TEBs, being especially careful not to compromise any TEB. k) Repeat steps for all the remaining COs' credentials on the list. **CO1: Frederico Neves** **Set # 2 TEB # BB02638534** **CO3: Ondrej Filip** **Set # 2 TEB # BB02638533** **CO4: Robert Seastrom** **Set # 2 TEB # BB02638532** **CO6 Successor: Hugo Salgado** **Set # 1 TEB # BB02638531** (CO reviews the card set prior to placing into TEB) **Set # 2 TEB # BB02638530** **CO7: Dileepa Lathsara** **Set # 2 TEB # BB02638529**		

CO	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	Set # 2 TEB # **BB02638534**	**Frederico Neves**		**2023 Apr __**		
CO3	Set # 2 TEB # **BB02638533**	**Ondrej Filip**		**2023 Apr __**		
CO4	Set # 2 TEB # **BB02638532**	**Robert Seastrom**		**2023 Apr __**		
CO6	Set # 1 TEB # **BB02638531** Set # 2 TEB # **BB02638530**	**Hugo Salgado**		**2023 Apr __**		
CO7	Set # 2 TEB # **BB02638529**	**Dileepa Lathsara**		**2023 Apr __**		

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

Step	Activity	Initials	Time
19	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
20	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.**		
21	SSC1 removes the safe log, then 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.**		
22	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 while showing it to the audit camera above, then place it inside Safe #1 　c) Write the date, time, and signature on the safe log where **"Return"** is indicated. 　d) IW verifies the safe log entry, then initials it. **HSM5E: TEB # BB51184606** **HSM6E: TEB # BB51184243** **Laptop3: TEB # BB97448418** **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638528** **KSK-2023: TEB # BB02638526**		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
23	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.		
24	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, and 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 is off.		
25	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
26	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)		
27	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.**		
28	SSC2 removes the safe log, then 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

29	COs perform the following steps sequentially to return the listed TEBs:
	    a) CO reads aloud the TEB number(s), then verifies integrity while showing the TEB(s) to the audit camera above
	    b) After the CA operates the guard key in the bottom lock, CO reads aloud the safe deposit box number and uses their tenant key to operate the top lock.
	Note: The COs will retrieve their new safe deposit box keys when specified below.
	    c) CO opens their safe deposit box, places their TEB(s) inside, then closes and locks the safe deposit box.
	    d) CO writes the date and time, then signs the safe log where **"Return"** is indicated.
	    e) IW verifies the completed safe log entry, then initials it.
	
	CO1: Frederico Neves
	Box # 1239
	Set # 2 TEB # BB02638534
	
	CO3: Ondrej Filip
	Box # 1241
	Set # 2 TEB # BB02638533
	
	CO4: Robert Seastrom
	Box # 1243
	Set # 2 TEB # BB02638532
	
	CO6 Successor: Hugo Salgado
	Box # 1242 (Retrieve keys from lock)
	Set # 1 TEB # BB02638531
	Set # 2 TEB # BB02638530
	
	CO7: Dileepa Lathsara
	Box # 1263
	Set # 2 TEB # BB02638529		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
30	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.		
31	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and 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 is off.		
32	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).		

Act 9: 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
- Ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Prepare the audit bundle materials

Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.		
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. **All signatories declare that this script is a true and accurate record of the ceremony.** All attendees may sign to attest the **Root KSK 2023** generation output log.		
3	CA reviews IW's script, then signs the participants list.		
4	IW signs the list and records the completion time.		

Retiring Crypto Officers

Step	Activity	Initials	Time
5	CA acknowledges all retiring Crypto Officers and presents them with a token of our appreciation. **Gaurab Upadhaya**		

Stop Online Streaming and Recording

Step	Activity	Initials	Time
6	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.		
7	CA requests that an SA stop the audit camera video recording.		
8	CA informs onsite participants of post ceremony activities.		
9	Ceremony participants take a group photo.		

Sign Out of Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
10	RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.) SA, IW, and CA must remain in Tier 4 (Key Ceremony Room.)		

Bundle Audit Materials

Step	Activity	Initials	Time
11	IW makes a copy of their script for off-site audit bundle containing: a) Output of signer system - HSMFD. b) Copy of IW's key ceremony script. c) Audio-visual recording from the audit cameras. d) Logs from the Physical Access Control System and Intrusion Detection System: Range: **20221103 00:00:00 to 20230428 00:00:00 UTC** e) IW's attestation (See Appendix C on page 42). f) SA's attestation (See Appendix D on page 43 and Appendix E on page 44). All TEBs are labeled **Root DNSSEC KSK Ceremony 49**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.		

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-1.0.0coen_amd64.deb
A debian package is an **ar** archive. To extract data from a deb package, use the command **ar -x ksk-tools-1.0.0coen_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

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 42.

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 43.

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 44. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Other items

If applicable.

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: **Patrick Jones**

Signature:

_____

Date: 2023 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: **20221103 00:00:00 to 20230428 00:00:00 UTC.**

SA:

Signature:

Date: 2023 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 6th Edition (2020-11-04). No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA: _____

Signature: _____

Date: 2023 Apr __