Root DNSSEC KSK Ceremony 43

Thursday 14 October 2021

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	Joe Catapano / ICANN			
CO4	Robert Seastrom			
CO5	Christopher Griffiths		2021 Oct —	
CO6	Gaurab Upadhaya			
SA	Sean Freeark / ICANN			
SA	Darren Kara / ICANN			
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 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 DVD, etc
• Safe #2: The COs' smartcards 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.		
4	CA confirms that additional required personnel including COs, RZM, and Auditors are connected to the remote call. Scheduled remote participants are: **CO2: Anne-Marie Eklund Lowinder** (Key designated as backup) **RZM: Duane Wessels / Verisign** **RZM: Trevor Davis / Verisign** **AUD: Paul M Lee / RSM** **Note 1: The CO2 Anne-Marie Eklund Lowinder Safe Deposit Box Key TEB # BB91951321 has been designated as a backup. See Appendix F on page 43.** **Note 2: The COs' tenant key was individually transmitted to a trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.**		

Emergency Evacuation Procedures and Electronics Policy

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

Verify the Time and Date

Step	Activity	Initials	Time
8	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
9	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)		
10	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.**		
11	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 Extract the Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
12	COs perform the following steps sequentially to retrieve the required TEBs: a) After the CA operates the guard key in the bottom lock, CO uses their tenant key to operate the top lock and open their assigned safe deposit box. b) CO reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB. c) CO reads aloud the TEB numbers, then verifies their integrity while showing them to the audit camera above. d) CO retains the TEB(s) specified below, then locks the safe deposit box. e) CO writes the date and time, then signs the safe log where **"Remove"** is indicated. f) IW verifies the completed safe log entries, then initials it. **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584402 (Retain)** **SO TEB # BB46584401 (Retain)** **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46584439 (Retain)** **SO TEB # BB46584440 (Retain)** **CO6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB46584441 (Retain)** **SO TEB # BB46584442 (Retain)**		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
13	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.		
14	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.		
15	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
16	CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.)		
17	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.**		
18	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
19	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, time, and signature on the safe log where **"Remove"** is indicated. e) IW verifies the safe log entry, then initials it. **HSM4: TEB # BB51184675 (Check and Return)** *Last Verified: KSK Ceremony 43-AC3 2021-06-10* **HSM5E: TEB # BB51184674 (Place on Cart)** *Last Verified: KSK Ceremony 43-AC3 2021-06-10* **HSM6E: TEB # BB51184245 (Place on Cart)** *Last Verified: KSK Ceremony 43-AT 2021-10-13* **Laptop3: TEB # BB81420111 (Check and Return)** *Last Verified: KSK Ceremony 39 2019-11-14* **Laptop4: TEB # BB81420106 (Place on Cart)** *Last Verified: KSK Ceremony 37 2019-05-16* **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584443 (Place on Cart)** *Last Verified: KSK Ceremony 39 2019-11-14* **KSK-2017: TEB # BB46584393 (Place on Cart)** *Last Verified: KSK Ceremony 37 2019-05-16* **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
20	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.		
21	SSC1 returns the safe log back 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.		
22	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		

Act 2: Equipment Setup

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

- Boot the laptop using the OS DVD (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 # BB51184674 / Serial # H1903018** *Last Verified: KSK Ceremony 43-AC3 2021-06-10* **Laptop4: TEB # BB81420106 / Service Tag # 58SVSG2** *Last Verified: KSK Ceremony 37 2019-05-16* **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584443** *Last Verified: KSK Ceremony 39 2019-11-14* **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.**		
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 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) Immediately insert the **OS DVD 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 DVD 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 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 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 DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/43		

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 "20211014 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 39 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 2019/11/14
	
	  # find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist
	
	  SHA-256: 51368713ada32cedea1f0c9ab34d1b30c842bc6f8e46d6467e85db2128deeb6b
	  PGP Words: drunken congregate Neptune barbecue ringbolt pandemic Burbank unify Trojan busi
	  nessman ammo newsletter scallion disruptive beeswax commando spaniel December showgirl hemi
	  sphere orca detergent stockman detergent locale leprosy suspense Camelot breadline telephon
	  e trouble Hamilton
	
	IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 39 annotated script.		

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 39** 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-20211014.log`		

Start the HSM Activity 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) Ensure an RJ45 blockout is present in the **"MGMT"** port of the HSM. Install one if not present. c) Plug the null modem cable into the serial port of the HSM. d) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H1903018**, then scroll back to the bottom. **HSM5E: Serial # H1903018** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

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

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

- The CA activates the HSM using the COs' smartcards
- After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop
- The ksrsigner application uses the private key stored in the HSM to generate the SKR containing the digital signatures of the ZSK slated for future use
- The CA then prints the signer log, backs up the newly created SKR, and deactivates the HSM

Crypto Officer Credentials Check

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. b) CO and CA open the TEB, then the CA removes the plastic case containing the card(s). c) CA opens the plastic case, then places the card(s) within on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table. **CO4: Robert Seastrom** **OP TEB # BB46584402** **SO TEB # BB46584401** **CO5: Christopher Griffiths** **OP TEB # BB46584439** **SO TEB # BB46584440** **CO6: Gaurab Upadhaya** **OP TEB # BB46584441** **SO TEB # BB46584442**		

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. 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 FD labeled **"KSR"** 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 2022 Q1

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: **ksrsigner /media/KSR/KSK43/ksr-root-2022-q1-0.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 2022 Q1

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 themself. 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) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.		
9	Participants confirm that the hash displayed on the terminal window 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/KSR/KSK43/skr-root-2022-q1-0.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) **lpadmin -p HP -o copies-default=X** **Note: Replace "X" with the amount of copies needed for the participants.** b) **printlog ksrsigner-202110*.log**		
12	IW attaches a copy of the required ksrsigner log to their script.		

Back up 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/KSR** b) Copy the contents of the KSRFD to the HSMFD by executing: **cp –pR /media/KSR/* .** **Note: Confirm overwrite by entering "y" if prompted.** c) List the contents of the HSMFD to verify it has been copied successfully by executing: **ls –ltrR** d) Unmount the KSRFD by executing: **umount /media/KSR**		
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.**		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
15	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 displays the HSM activity logging 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. 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.**		

Act 4: Issue Temporary CO, AAK, and SMK Cards

When a ceremony includes the introduction of a new HSM, it is necessary to generate temporary cards to allow importing of an existing KSK backup into the new HSM, and for existing CO credentials to perform signing and administrative operations in the new HSM. These temporary cards will be used and subsequently destroyed before the completion of the ceremony.

The CA will generate the required material to introduce a new HSM by performing the steps below:

• Generate CO cards for use with the cryptographic menu functions in the new HSM
• Generate AAK cards to allow the currently issued CO credentials to function in the new HSM
• Generate SMK cards to allow an existing KSK backup to be imported into the new HSM

Issue Temporary Crypto Officer (CO) Cards

Step	Activity	Initials	Time
1	CA selects the **HSM Output** terminal window.		
2	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to issue Crypto Officer (CO) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"1.Issue Cards"**, press **ENT** to confirm. h) Select **"1.Issue CO Cards"**, press **ENT** to confirm. i) When **"Issue CO Cards?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. k) When **"Num Req Cards?"** is displayed, enter **"2"**, then press **ENT**. l) When **"Insert Card #X?"** is displayed, insert the required CO card. m) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. n) When **"Remove Card?"** is displayed, remove the CO card. o) Repeat steps l) to n) for the 2nd CO card. p) When **"CO Cards Issued"** is displayed, press **ENT** to confirm. q) Press **CLR** to return to the menu **"Role Mgmt"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Issue Temporary Authorization Key (AAK) Cards

Step	Activity	Initials	Time
3	CA performs the following steps to issue Adapter Authorization Key (AAK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.Backup AAK"** from the same menu **"Role Mgmt"**, press **ENT** to confirm. c) When **"Backup AAK?"** is displayed, press **ENT** to confirm. d) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. e) When **"Insert Card #X?"** is displayed, insert the required AAK card. f) When **"Remove Card?"** is displayed, remove the AAK card. g) Repeat steps e) to f) for the 2nd AAK card. h) When **"AAK Exported"** is displayed, press **ENT** to confirm. i) Press **CLR** to return to the 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.**		

Issue Temporary Storage Master Key (SMK) Cards

Step	Activity	Initials	Time
4	CA performs the following steps to issue Storage Master Key (SMK) cards: 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 CO card. g) Select **"4.SMK"**, press **ENT** to confirm. h) Select **"2.Backup SMK"**, press **ENT** to confirm. i) When **"Backup SMK?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"4"**, then press **ENT**. k) When **"Num Req Cards?"** is displayed, enter **"2"**, then press **ENT**. l) When **"Insert Card #X?"** is displayed, insert the required SMK card. m) When **"Remove Card?"** is displayed, remove the SMK card. n) Repeat steps l) to m) for the 2nd, 3rd and 4th SMK cards. o) When **"Verify Card #X?"** is displayed, insert the required SMK card. p) When **"Remove Card?"** is displayed, remove the SMK card. q) Repeat steps o) to p) for the 2nd, 3rd and 4th SMK cards. r) When **"SMK Backed Up"** is displayed, press **ENT** to confirm. s) Press **CLR twice** 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.**		

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
5	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.**		
6	CA places the HSM into a prepared TEB, then seals it.		

7	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 # BB51184241 / Serial # H1903018		

Act 5: Introduce New HSM

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

- Verify new HSM serial number
- Import the Adapter Authorization Key (AAK)
- Configure the HSM to Secure State
- Change and verify API settings
- Import Storage Master Key (SMK)
- Import App Key
- Verify connectivity, activate, and initialize HSM
- Destroy temporary credential cards

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the new 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. e) Plug the null modem cable into the serial port of the HSM. f) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** g) Scroll the logging screen up and locate the HSM serial number. h) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. i) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **HSM6E: TEB # BB51184245 / Serial # H2001001** **Last Verified: KSK Ceremony 43-AT 2021-10-13** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.** **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.**		

Import the AAK

Step	Activity	Initials	Time
2	CA performs the following steps to import the Adapter Authorization Key (AAK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Restore AAK"**, press **ENT** to confirm. c) When **"Restore AAK?"** is displayed, press **ENT** to confirm. d) When **"Insert Card #X?"** is displayed, insert the required AAK card. e) When **"Remove Card?"** is displayed, remove the AAK card. f) Repeat steps d) to e) for the 2nd AAK card. g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm. 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.**		

Configure the HSM to Secure State

Step	Activity	Initials	Time
3	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.Secure"**, press **ENT** to confirm. c) When **"Secure?"** is displayed, 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 cards. h) When **"SMK AES Triple DES?"** is displayed, press **CLR** to skip. i) When **"SMK AES"** is displayed, press **ENT** to confirm. j) When **"LAN Port Number?"** is displayed, press **CLR** to skip. k) When **"Enable IPv4/IPv6?"** is displayed, press **CLR** to skip. l) When **"LAN IPv4 Address?"** is displayed, press **CLR** to skip. m) When **"LAN IPv4 Mask?"** is displayed, press **CLR** to skip. n) When **"Set IPv4 Gateway?"** is displayed, press **CLR** to skip. o) When **"LAN IPv6 Address?"** is displayed, press **CLR** to skip. p) When **"LAN IPv6 Mask?"** is displayed, press **CLR** to skip. q) When **"Set IPv6 Gateway?"** is displayed, press **CLR** to skip. r) When **"Remote Mgmt Off Enable?"** is displayed, press **CLR** to skip. s) When **"Remote Mgmt Off** is displayed, press **ENT** to confirm. t) When **"Change Clock?"** is displayed, press **CLR** to skip. u) When **"Import Config?"** is displayed, press **CLR** to skip. v) When **"FIPS Mode On Disable?"** is displayed, press **CLR** to skip. w) When **"FIPS Mode On"** is displayed, press **ENT** to confirm. x) When **"Global Key Export Enabled"** is displayed, press **CLR** to skip. **Done Rebooting Device** will be displayed. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # _____ 1st SO card _____ of 7 2nd SO card _____ of 7 3rd SO card _____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Change the API Settings

Step	Activity	Initials	Time

4	CA performs the following steps to change the API settings:
	    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 CO card.
	    g) Select **"5. API Settings"**, press **ENT** to confirm.
	    h) Select **"1.Key Import"**, press **ENT** to confirm.
	    i) When **"Key Import On Disable?"** is displayed, press **ENT** to confirm.
	    j) Select **"2.Key Export"**, press **ENT** to confirm.
	    k) When **"Key Export On Disable?"** is displayed, press **ENT** to confirm.
	    l) Select **"5.Sym Key Der"**, press **ENT** to confirm.
	    m) When **"Sym Key Der On Disable?"** is displayed, press **ENT** to confirm.
	    n) Press **CLR twice** 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.		

Verify API Settings

Step	Activity	Initials	Time

5	CA performs the following steps to dump the status of the HSM:
	    a) Utilize the HSM's keyboard to scroll through the menu using < >
	    b) Select **"4.HSM Info"**, press **ENT** to confirm.
	    c) Select **"8.Output Info"**, press **ENT** to confirm.
	    d) When **"Output Info?"** is displayed, press **ENT** to confirm.
	    e) Press **CLR** to return to the main menu **"Secured"**.
	
	CA selects the **HSM Output** terminal window and scrolls up to confirm with IW the output of the HSM configuration matches with the list below:
	
	`Modes: (1=Enabled 0=Disabled)`
	`Global Key Export 1`
	`App Key Import 0`
	`App Key Export 0`
	`Asymmetric Key Gen 1`
	`Symmetric Key Gen 1`
	`Symmetric Key Derive 0`
	`Signing 1`
	`Signature Verify 1`
	`MAC Generation 1`
	`MAC Verification 1`
	`Encrypt / Decrypt 1`
	`Delete Asym Key 1`
	`Delete Sym Key 1`
	`Output Key Details 1`
	`Output Key Summary 1`
	`Suite B Algorithms 1`
	`Non Suite B Algs 1`
	`Auto Online 0`
	`Remote Management 0`
	`AES SMK`
	`Set Offline`
	`FIPS Mode`		

App Key Backups

Step	Activity	Initials	Time
6	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) Remove and discard the TEB, then place the backup HSMFD on its designated area of the ceremony table. e) Using a sharpie, write **1** and **2** respectively on the App key cards, then place them on the designated card holder. **KSK-2017: TEB # BB46584393** **Last Verified: KSK Ceremony 37 2019-05-16** 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.		

Import the SMK and the KSK

Step	Activity	Initials	Time

7	CA performs the following steps to import Storage Master Key (SMK):
	    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 CO card.
	    g) Select **"4.SMK"**, press **ENT** to confirm.
	    h) Select **"3.Restore SMK"**, press **ENT** to confirm.
	    i) When **"Restore SMK?"** is displayed, press **ENT** to confirm.
	    j) When **"Insert Card SMK #X?"** is displayed, insert the SMK card.
	    k) When **"Remove Card?"** is displayed, remove the SMK card.
	    l) Repeat steps j) to k) for the 2nd SMK card.
	    m) When **"SMK Restored"** is displayed, press **ENT** to confirm.
	    n) Press **CLR** to return to the main menu **"Key Mgmt"**.
	
	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.		

8	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 same menu **"Key Mgmt"**, 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 twice** to return to the main menu **"Secured"**.
	
	IW records which card was used below. Card is returned to its designated card holder after use.
	App Key card _____
	
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

Return the KSK into a TEB

Step	Activity	Initials	Time
9	CA places the KSK and the backup HSMFD into a prepared TEB, then seals it.		

10	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 matches 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 KSK TEB on the cart.
	
	KSK-2017: TEB # BB91951367		

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
11	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. 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
12	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		

13	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 Copy of the KSRFD

Step	Activity	Initials	Time
14	CA plugs the FD labeled **"KSR_COPY"** 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 2022 Q1

Step	Activity	Initials	Time
15	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml`		
16	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 2022 Q1

Step	Activity	Initials	Time
17	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.		
18	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"**		
19	CA enters **"y"** in response to **"Is this correct (y/N)?"** to complete the KSR signing operation. The SKR is located in: **/media/KSR_COPY/KSK43/skr-root-2022-q1-0.xml**		

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
20	CA executes the commands below using the terminal window to print the KSR Signer log: a) **lpadmin -p HP -o copies-default=X** **Note: Replace "X" with the amount of copies needed for the participants.** b) **printlog ksrsigner-202110*.log**		
21	IW attaches a copy of the required ksrsigner log to their script.		

Verification of the Hash of the SKR Copy

Step	Activity	Initials	Time
22	CA read the SHA256 hash in PGP wordlist format for the generated SKR and the ceremony participants match the hash with the previous SKR.		

Remove Copy of the KSRFD

Step	Activity	Initials	Time
23	CA executes the following commands using the terminal window: a) List the contents of the KSRFD by executing: **ls –ltrR /media/KSR_COPY** b) Unmount the KSRFD by executing: **umount /media/KSR_COPY**		
24	CA removes the **KSR_COPY** containing the SKR files, then gives it to IW for audit purpose.		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
25	CA selects the **HSM Output** terminal window and presses the **RESTART** button on the HSM to make it offline and waits for the self test to complete. Confirm the **"READY"** LED on the HSM is **OFF**.		

Clear and Destroy SMK Cards

Step	Activity	Initials	Time

26	CA performs the following steps to clear Storage Master Key (SMK) cards:
	    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 CO card.
	    g) Select **"4.SMK"**, press **ENT** to confirm.
	    h) Select **"4.Clear Cards"**, press **ENT** to confirm.
	    i) When **"Clear Card?"** is displayed, press **ENT** to confirm.
	    j) When **"Insert Card SMK 1?"** is displayed, take the **SMK #1** card from the cardholder, show the **SMK #1** card to the audit camera and then insert the **SMK #1** card into the HSM's card reader.
	    k) When **"Num Cards?"** is displayed, enter **"4"**, then press **ENT**.
	    l) When **"Are you sure?"** is displayed, press **ENT** to confirm.
	    m) When **"Remove Card?"** is displayed, remove the SMK card.
	    n) When **"Insert Card SMK #X?"** is displayed, take the **SMK #X** card from the cardholder, show the **SMK #X** card to the audit camera and then insert the **SMK #X** card into the HSM's card reader.
	    o) When **"Are you sure?"** is displayed, press **ENT** to confirm.
	    p) When **"Remove Card?"** is displayed, remove the SMK card.
	    q) Repeat steps n) to p) for the 3rd and 4th SMK cards.
	    r) Press **CLR twice** to return to the main menu **"Secured"**.
	    s) CA uses the shredder to destroy the cleared SMK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

Clear and Destroy CO and AAK Cards

Step	Activity	Initials	Time

27	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to clear Crypto Officer (CO) cards:
	    a) Utilize the HSM's keyboard to scroll through the menu using < >
	    b) Select **"7.Role Mgmt"**, press **ENT** to confirm.
	    c) When **"Insert Card SO #X?"** is displayed, insert the SO card.
	    d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.
	    e) When **"Remove Card?"** is displayed, remove the SO card.
	
	    f) Repeat steps c) to e) for the 2nd and 3rd SO card.
	    g) Select **"4.Clear RoleCard"**, press **ENT** to confirm.
	    h) When **"Clear Card?"** is displayed, press **ENT** to confirm.
	    i) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**.
	    j) When **"Insert Card #X?"** is displayed, take the required **CO #X** card from the cardholder, show the **CO #X** card to the audit camera and then insert the **CO #X** card into the HSM's card reader.
	    k) When **"Are you sure?"** is displayed, press **ENT** to confirm.
	    l) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.
	    m) When **"Remove Card?"** is displayed, remove the CO card.
	
	    n) Repeat steps j) to m) for the 2nd CO card.
	
	IW records which cards were used below. Each card is returned to its designated card holder after use.
	Set # _____
	1st SO card _____ of 7
	2nd SO card _____ of 7
	3rd SO card _____ of 7
	
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

28	CA performs the following steps to clear Adapter Authorization Key (AAK) cards:
	    a) Utilize the HSM's keyboard to scroll through the menu using < >
	    b) Select **"5.Clear AAK Card"** from the same menu **"Role Mgmt"**, press **ENT** to confirm.
	    c) When **"Clear AAK Card?"** is displayed, press **ENT** to confirm.
	    d) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**.
	    e) When **"Insert Card AAK #X?"** is displayed, take the **AAK #X** card from the cardholder, show the **AAK #X** card to the audit camera and then insert the **AAK #X** card into the HSM's card reader.
	    f) When **"Are you sure?"** is displayed, press **ENT** to confirm.
	    g) When **"Remove Card?"** is displayed, remove the AAK card.
	
	    h) Repeat steps e) to g) for the 2nd AAK card.
	    i) Press **CLR** 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.		

29	CA uses the shredder to destroy the cleared CO and AAK 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
30	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.**		
31	CA places the HSM into a prepared TEB, then seals it.		

32	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 # BB51184242 / Serial # H2001001		

Act 6: Secure Hardware

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

- Back up 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' smartcards 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.**		

Prepare blank FDs and back up the HSMFD Contents

Step	Activity	Initials	Time
2	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: `shopt –s dotglob`		
3	CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content: a) `lpadmin -p HP -o copies-default=2` b) `hsmfd-hash –p` **Note: One copy for audit bundle and one copy for HSMFD package.**		
4	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls –ltrR`		
5	CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs: `mkdir /media/HSMFD1`		
6	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.		
7	CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: `df`		
8	CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD: a) `umount /dev/sdc1` b) `mkfs.vfat -n HSMFD -I /dev/sdc1` c) `mount /dev/sdc1 /media/HSMFD1` d) `cp -pR * /media/HSMFD1`		
9	CA executes the commands below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy, then unmounts the flash drive before removal: a) `hsmfd-hash -m` b) `umount /media/HSMFD1`		
10	CA removes the **HSMFD copy**, then places it on the holder. **Wait for the activity light on the backup HSMFD to stop flashing before removal.**		
11	CA repeats step 6 to 10 for the 2nd copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**		
12	CA repeats step 6 to 10 for the 3rd copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**		
13	CA repeats step 6 to 10 for the 4th copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**		
14	CA repeats step 6 to 10 for the 5th copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**		

Print Logging Information

Step	Activity	Initials	Time
15	CA executes the following commands using the terminal window to print a copy of the logging information: a) `lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true` b) `enscript -2Gr script-202110*.log` c) `enscript -Gr --font="Courier8" ttyaudit-tty*-202110*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**		

Place HSMFDs and OS DVDs into a TEB

Step	Activity	Initials	Time
16	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.		
17	CA performs the following steps to switch OFF the laptop and remove the OS DVD: a) Remove the OS DVD from the laptop. b) Turn OFF the laptop by pressing the power button. c) Disconnect all connections from the laptop.		
18	CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it.		
19	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 DVD TEB on the cart. **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951368**		
20	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).		

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.		

22	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.
	
	Laptop4: TEB # BB81420124 / Service Tag # 58SVSG2		

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time

23	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps:
	    a) CA takes the OP TEB and plastic case prepared for the CO.
	    b) CO takes their OP card from the card holder and places it inside the plastic case.
	    c) CO gives the plastic case containing the OP card to the CA.
	    d) CA places the plastic case into the prepared 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 card to the CO.
	    h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen.
	    i) Repeat steps a) to h) for the 2 SO cards respectively, ensuring they're facing outward in the plastic case and placed into the prepared SO TEB.
	    j) CO writes the date and time, then signs the table of IW's script, then IW initials the entry.
	    k) CO returns to their seat with their credentials, being especially careful not to compromise any TEB.
	    l) Repeat steps for all the remaining COs on the list.
	
	CO4: Robert Seastrom
	OP TEB # BB91951237
	SO TEB # BB91951236
	
	CO5: Christopher Griffiths
	OP TEB # BB91951235
	SO TEB # BB91951234
	
	CO6: Gaurab Upadhaya
	OP TEB # BB91951233
	SO TEB # BB91951232		

CO	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO4	OP 4 of 7 SO 4 of 7	OP TEB # **BB91951237** SO TEB # **BB91951236**	**Robert Seastrom**		**2021 Oct __**		
CO5	OP 5 of 7 SO 5 of 7	OP TEB # **BB91951235** SO TEB # **BB91951234**	**Christopher Griffiths**		**2021 Oct __**		
CO6	OP 6 of 7 SO 6 of 7	OP TEB # **BB91951233** SO TEB # **BB91951232**	**Gaurab Upadhaya**		**2021 Oct __**		

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

Step	Activity	Initials	Time
24	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
25	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.**		
26	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.**		

27	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 # BB51184241
	HSM6E: TEB # BB51184242
	Laptop4: TEB # BB81420124
	OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951368
	KSK-2017: TEB # BB91951367		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
28	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.		
29	SSC1 returns the safe log back 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.		
30	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
31	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)		
32	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.**		
33	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
34	COs perform the following steps sequentially to return the required 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 uses their tenant key to operate the top lock and open their safe deposit box. c) CO reads aloud the safe deposit box number, places their TEB(s) inside, then 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. **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB91951237** **SO TEB # BB91951236** **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB91951235** **SO TEB # BB91951234** **CO6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB91951233** **SO TEB # BB91951232**		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
35	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.		
36	SSC2 returns the safe log back 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.		
37	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
- 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.**		
3	CA reviews IW's script, then signs the participants list.		
4	IW signs the list and records the completion time.		

Stop Online Streaming and Post Ceremony Information

Step	Activity	Initials	Time
5	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.		
6	CA informs onsite participants of post ceremony activities.		
7	Ceremony participants take a group photo.		

Sign Out of Tier 4 (Key Ceremony Room) and Stop Recording

Step	Activity	Initials	Time
8	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.)		
9	CA requests that an SA stop the audit camera video recording.		

Bundle Audit Materials

Step	Activity	Initials	Time
10	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: **20191114 00:00:00 to 20211015 00:00:00 UTC** e) IW's attestation (See Appendix C on page 40). f) SA's attestation (See Appendix D on page 41 and Appendix E on page 42). All TEBs are labeled **Root DNSSEC KSK Ceremony 43**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.		

Appendix A: References

The numeric items listed below has been referenced in the script.

[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] **sha2wordlist:** Is an application written in C by Kirei AB, which digests STDIN and output a SHA-256 checksum displayed as PGP words.
The source code is available at https://github.com/kirei/sha2wordlist

[3] **configure-printer:** Is a bash script used to install the HP LaserJet printer from the command line instead using system-config-printer.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

[4] **hsmfd-hash:** Is a bash script used to calculate, print and compare SHA-256 checksums for the HSMFD flash drives. It has the following options:

    a) **-c Calculate the HSMFD SHA-256 hash and PGP Word List**
    b) **-p Print the calculated HSMFD SHA-256 hash and PGP Word List using the default printer**
    c) **-m Compare the calculated SHA-256 hashes between HSMFDs**

The following is the main command invoked by this script:
find -P */media/HSMFD/* **-type f -print0 | sort -z | xargs -0 cat | sha2wordlist**

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

The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

[5] **ttyaudit:** Is a perl script use to capture and logging the *HSM* output.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

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

[7] **ksrsigner:** Is an application written in C by Dr. Richard Lamb, which 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

[8] **printlog:** Is a bash script use to print the *Key Signing Log* output from **ksrsigner** application.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

[9] **keybackup:** Is an application written in C by Dr. Richard Lamb, which list, delete, and backup keys.
The source code is available at https://github.com/iana-org/dnssec-keytools

---

* A debian package is an **ar** archive. To extract data from a deb package, use the command **ar -x ksk-tools-0.1.0coen_amd64.deb**
Then extract the files with **tar -zxvf data.tar.xz**
The file will be located in the directory: **./opt/icann/bin/**

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 during the ceremony and attestation. See Appendix C on page 40.

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 41.

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 42. 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: 2021 Oct __

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: 20191114 00:00:00 to 20211015 00:00:00 UTC.

SA:

    _____

Signature:

      _____

Date: 2021 Oct __

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: 2021 Oct __

Appendix F: CO2 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO2 Anne-Marie Eklund Lowinder** Safe Deposit Box **Key TEB #BB91951321** dispatched from the CO.

This key has been designated as a backup. The TEB will remain sealed in the courier envelope unless the situation dictates its use. It will be sent back to the CO after the ceremony in its sealed state post-ceremony.

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with potentially less than the standard minimum of three Crypto Officers in-person, I, Anne-Marie Eklund Löwinder, am hereby entrusting my safe deposit box key enclosed in TEB # *BB 91951321* for safe deposit box #1259 located within Safe #2 at the key management facility in Culpeper, VA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it may be required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name *Anne-Marie Eklund Lowinder*

Signature *Anne-Marie Eklund Löwinder*

Date *2021-09-23*