

Root DNSSEC KSK Ceremony 52

Wednesday 14 February 2024

Root Zone KSK Operator Key Management Facility
1920 East Maple Avenue, El Segundo, CA 90245, 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	Francisco Arias / ICANN		2024 Feb —	
IW	Jonathan Denison / ICANN			
SSC1	Sabrina Tanamal / PTI			
SSC2	Hilary Jin / ICANN			
CO1	Arbogast Fabian			
CO2	Ralf Weber			
CO5	Ólafur Guðmundsson			
CO6	Jorge Etges			
RZM	Duane Wessels / Verisign			
RZM	Poonam Garg / Verisign			
AUD	Melanie Chen / RSM			
AUD	Grant An / RSM			
SA	Josh Jenkins / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Danielle Gordon / ICANN			
SW	Alireza Mohammadi / PTI			
SW	Seman Said / PTI			
EW	Nicholas Pelis			
EW	Alexander Bellos			

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

Instructions for a Root DNSSEC KSK Ceremony

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

Ceremony Guidelines:

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

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

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

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

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

Sign into Tier 4 (Key Ceremony Room)

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

Emergency Evacuation Procedures and Electronics Policy

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

Verify the Time and Date

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

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1.8	CA transports the guard key and flashlight, and with IW escorts SSC2 and the COs into Tier 5 (Safe Room.)		
1.9	SSC2 opens Safe #2 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.		
1.10	Perform the following steps to update the safe log: a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.		

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

Step	Activity	Initials	Time
1.11	<p>COs perform the following steps sequentially to access the listed TEBs:</p> <ul style="list-style-type: none"> a) After the CA operates the guard key in the lower lock, CO reads aloud their safe deposit box number then uses their tenant key to operate the upper lock. b) CO opens their safe deposit box, verifies its integrity, then removes the TEBs. c) CO reads aloud the TEB numbers, verifies integrity of TEBs, then presents them to the audit camera above. d) CO performs the actions specified below, locks their safe deposit box, and removes their key. e) CO writes the date and time, then signs the safe log. f) IW verifies the completed safe log entries, then initials them. g) CA locks the safe deposit box and removes the guard key. <p>CO1: Arbogast Fabian Box # 1788 Set # 1 TEB # BB02638503 (Check and Return) Last Verified: KSK Ceremony 50 2023-07-19 Set # 2 TEB # BB02638561 (Retain) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>CO2: Ralf Weber Box # 1071 Set # 1 TEB # BB02638504 (Check and Return) Last Verified: KSK Ceremony 50 2023-07-19 Set # 2 TEB # BB02638559 (Retain) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>CO5: Ólafur Guðmundsson Box # 1070 OP TEB # BB91951256 (Retain) SO TEB # BB02638563 (Retain) Set # 1 TEB # BB02638554 (Check and Return) Last Verified: KSK Ceremony 48 2023-02-01 Set # 2 TEB # BB02638553 (Retain) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>CO6: Jorge Etges Box # 1072 Set # 1 TEB # BB02638505 (Check and Return) Last Verified: KSK Ceremony 50 2023-07-19 Set # 2 TEB # BB02638551 (Retain) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1.12	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where " Close Safe " is indicated. IW verifies the entry then initials it.		
1.13	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, 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 adjacent to the Tier 5 (Safe Room) exit door is off.		
1.14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).		

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
1.15	CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.)		
1.16	SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.		
1.17	Perform the following steps to update the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where " Open Safe " is indicated. d) IW verifies the entry then initials it.		

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

Step	Activity	Initials	Time
1.18	CA performs the following steps to remove each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, verify its integrity, then present it to the audit camera above. c) Place each equipment TEB on the cart as specified in the list below. d) Write the date and time, then sign the safe log. e) IW verifies the completed safe log entries, then initials them.		
	HSM5W: TEB # BB51184282 (Check and Return) Last Verified: KSK Ceremony 50 2023-07-19		
	HSM6W: TEB # BB51184283 (Place on Cart) Last Verified: KSK Ceremony 50 2023-07-19		
	HSM7W: TEB # BB51184280 (Check and Return) Last Verified: KSK Ceremony 50 2023-07-19		
	HSM8W: TEB # BB51184549 (Place on Cart) Last Verified: AT Ceremony 52 2024-02-13		
	Laptop3: TEB # BB97448420 (Place on Cart) Last Verified: KSK Ceremony 48 2023-02-01		
	Laptop4: TEB # BB81420076 (Check and Return) Last Verified: KSK Ceremony 50 2023-07-19		
	OS media (release coen-1.0.0) + HSMFD: TEB # BB02638508 (Place on Cart) Last Verified: KSK Ceremony 50 2023-07-19		
	KSK-2017: TEB # BB02638568 (Place on Cart) Last Verified: KSK Ceremony 48 2023-02-01		
	KSK-2023: TEB # BB02638507 (Place on Cart) Last Verified: KSK Ceremony 50 2023-07-19		
<p>Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes. The shelves in the equipment safe can slide in and out for ease of use.</p>			

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

Step	Activity	Initials	Time
1.19	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the safe log entry then initials it.		
1.20	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, 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 adjacent to the Tier 5 (Safe Room) exit door is off.		
1.21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		

Act 2: 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
2.1	<p>CA performs the following steps to prepare the listed equipment:</p> <ol style="list-style-type: none"> Remove all equipment TEBs from the cart and place them on the ceremony table. Inspect each equipment TEB for tamper evidence. 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. Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. <p>HSM6W: TEB # BB51184283 / Serial # H2008009 Last Verified: KSK Ceremony 50 2023-07-19 Laptop3: TEB # BB97448420 / Service Tag # C8SVSG2 Last Verified: KSK Ceremony 48 2023-02-01 OS media (release coen-1.0.0) + HSMFD: TEB # BB02638508 Last Verified: KSK Ceremony 50 2023-07-19</p> <p>Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		
2.2	<p>CA performs the following steps to confirm that no hard drive and battery are in the laptop:</p> <ol style="list-style-type: none"> Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. Open the latch on the left side of the laptop to confirm that the battery slot is empty. 		
2.3	<p>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 # 2</p>		
2.4	<p>CA performs the following steps to boot the laptop:</p> <ol style="list-style-type: none"> Connect the USB printer cable into the rear USB port of the laptop. Connect the null modem cable into a USB port of the laptop. Connect the external HDMI display cable. Connect the power supply. Insert the OS media release coen-1.0.0 Copy # 2. Switch it ON. 		
2.5	<p>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</p>		

OS Media Checksum Verification

Step	Activity	Initials	Time
2.6	<p>Using the Commands terminal window, CA executes the following steps:</p> <ol style="list-style-type: none"> Verify the byte count of the SD card matches the ISO size by running the following command: <code>df -B1 /dev/sda</code> Calculate the SHA-256 hash by executing: <code>head -c 375431168 /dev/sda sha2wordlist</code> IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. <p>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.</p> <p>SHA-256 hash: 405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a</p> <p>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</p> <p>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/52</p>		

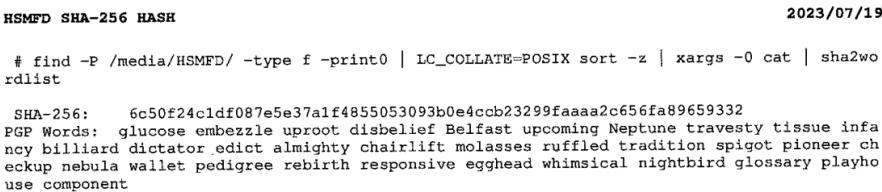
Printer Setup

Step	Activity	Initials	Time
2.7	<p>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: <code>configure-printer</code></p>		

Date Setup

Step	Activity	Initials	Time
2.8	<p>CA executes <code>date</code> using the terminal window to verify if the date/time reasonably matches the ceremony clock.</p> <p>If the date/time do not match, perform the following steps:</p> <ol style="list-style-type: none"> Execute <code>date -s "20240214 HH:MM:SS"</code> to set the time. where HH is two-digit hour, MM is two-digit minutes and SS is two-digit seconds. Execute <code>date</code> to confirm the date/time matches the clock. 		

Connect the HSMFD

Step	Activity	Initials	Time
2.9	CA plugs the Ceremony 50 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.		
2.10	Using the Commands terminal window, CA executes the command below to calculate the SHA-256 hash of the HSMFD: <code>hsmfd-hash -c</code> 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.  <p>The screenshot shows the following terminal output:</p> <pre>HSMFD SHA-256 HASH 2023/07/19 # find -P /media/HSMFD/ -type f -print0 LC_COLLATE=POSIX sort -z xargs -0 cat sha2wo rdlist SHA-256: 6c50f24c1df087e5e37a1f4855053093b0e4ccb23299faaaa2c656fa89659332 PGP Words: glucose embezzle uproot disbelief Belfast upcoming Neptune travesty tissue infa ncy billiard dictator edict almighty chairlift molasses ruffled tradition spigot pioneer ch eckup nebula wallet pedigree rebirth responsive egghead whimsical nightbird glossary playho use component</pre> IW confirms that the result matches the SHA-256 hash of the HSMFD using the printed HSMFD hash from the Ceremony 50 OS Media bundle.		

Distribute Previous HSMFD

Step	Activity	Initials	Time
2.11	CA gives the unused HSMFD 50 and the sheet of paper with the printed HSMFD hash to RKOS.		

Start the Terminal Session Logging

Step	Activity	Initials	Time
2.12	Using the Commands terminal window, CA executes the command below to change the working directory to HSMFD: <code>cd /media/HSMFD</code>		
2.13	CA executes the command below to log activities of the Commands terminal window: <code>script script-20240214.log</code>		

Start the HSM Output Logging

Step	Activity	Initials	Time
2.14	Using the HSM Output terminal window, CA performs the following steps to capture the activity logs of the HSM: a) Change the working directory to HSMFD by executing: <code>cd /media/HSMFD</code> b) Set the serial port baud rate by executing: <code>stty -F /dev/ttyUSB0 115200</code> c) Start logging the serial output by executing: <code>ttyaudit /dev/ttyUSB0</code> Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.		

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
2.15	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none"> a) Verify the label on the HSM reads HSM6W. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. <p>Note: Status information should appear in the HSM output terminal window.</p> <ul style="list-style-type: none"> d) Scroll up on the terminal window while IW verifies the displayed HSM serial number on the screen reads H2008009. e) Scroll down to the end of the terminal window. <p>HSM6W: Serial # H2008009</p> <p>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</p>		

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

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

- The CA activates the HSM using the Crypto Officers' credentials
- After connectivity is confirmed, the flash drive containing the KSRs is inserted into the laptop
- The ksr signer application uses the private key stored in the HSM to generate the SKRs containing the digital signatures of the ZSK slated for future Root Zone signing
- The CA prints the signer log, backs up the newly generated SKRs, and deactivates the HSM

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
3.1	<p>The CA calls each of the COs listed below sequentially to perform the following steps:</p> <ul style="list-style-type: none"> a) CO reads aloud the TEB number, then CA inspects it for tamper evidence while the IW verifies its "last verified" information using the specified previous ceremony script. b) CO and CA open the TEB, then the CA removes the credential case to perform the action specified below. <p>CO1: Arbogast Fabian Set # 2 TEB # BB02638561 (CO places cards on their designated card holders) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>CO2: Ralf Weber Set # 2 TEB # BB02638559 (CO places cards on their designated card holders) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>CO5: Ólafur Guðmundsson OP TEB # BB91951256 (CA sets the plastic case with cards aside for destruction) (Last Verified: KSK Ceremony 44 2022-02-16) SO TEB # BB02638563 (CA sets the plastic case with cards aside for destruction) (Last Verified: KSK Ceremony 48 2023-02-01) Set # 2 TEB # BB02638553 (CO places cards on their designated card holders) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>CO6: Jorge Etges Set # 2 TEB # BB02638551 (CO places cards on their designated card holders) Last Verified: KSK Ceremony 48 2023-02-01</p> <p>Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
3.2	<p>CA performs the following steps to activate the HSM:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>Set # 2 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
3.3	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		
3.4	<p>CA performs the following steps to test the network connectivity between laptop and HSM:</p> <ul style="list-style-type: none"> a) Select the Commands terminal window b) Test connectivity by executing: <code>ping hsm</code> c) Wait for responses, then exit by pressing: <code>Ctrl + C</code> 		

Insert the KSRFD

Step	Activity	Initials	Time
3.5	<p>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.</p> <p>Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.</p>		

Execute the KSR Signer for KSR 2024 Q2

Step	Activity	Initials	Time
3.6	Using the Commands terminal window, the CA executes the command below to change the directory: <code>cd /media/KSRFD/KSK52/</code>		
3.7	Using the Commands terminal window, the CA executes the command below to sign the KSR file: <code>kskm-ksrsigner</code>		

Verify the KSR Hash for KSR 2024 Q2

Step	Activity	Initials	Time
3.8	<p>When the hash of the KSR is displayed in the terminal window, perform the following:</p> <p>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.</p> <p>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.</p> <p>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:</p> <p>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.</p> <p>_____</p> <p>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.</p>		
3.9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks "are there any objections?"		
3.10	CA enters Yes in response to "Sign KSR?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSREFD/KSK52/skr-root-2024-q2-0.xml</code>		

Print Copies of the KSR Signer Log

Step	Activity	Initials	Time
3.11	<p>Using the Commands terminal window, the CA executes the commands below to print the KSR Signer log:</p> <p>a) <code>printlog kskm-ksrsigner-202402*.log X</code></p> <p>Note: Replace "X" with the amount of copies needed for the participants.</p>		
3.12	IW attaches a copy of the required ksr signer log to their script.		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
3.13	<p>CA deactivates the HSM by performing the following steps: Note: CA will use OP cards not previously utilized in this ceremony if available.</p> <ol style="list-style-type: none"> CA selects the HSM Output terminal window. Utilize the HSM's keyboard to scroll through the menu using < > Select "2.Set Offline", press ENT to confirm. When "Set Offline?" is displayed, press ENT to confirm. When "Insert Card OP #X?" is displayed, insert the OP card from the card holder. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the OP card. Repeat steps e) to g) for the 2nd and 3rd OP cards. <p>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.</p> <p>Set # 2 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

OS Media Checksum Verification

Step	Activity	Initials	Time
3.14	<p>Using the Commands terminal window, CA executes the following steps:</p> <ol style="list-style-type: none"> Verify the byte count of the SD card matches the ISO size by running the following command: <code>df -B1 /dev/sda</code> Calculate the SHA-256 hash by executing: <code>head -c 375431168 /dev/sda sha2wordlist</code> IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. <p>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.</p> <p>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</p> <p>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/52</p>		

Act 4: Destroy OP and SO Cards

Operator (OP) and Security Officer (SO) cards were originally issued in 2010 and these original cards have reached the end of their operational period. New OP and SO card sets were previously generated as replacements, so the original cards are safe to destroy.

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
4.1	<p>CA performs the following steps to clear Operator (OP) and Security Officer (SO) cards:</p> <ol style="list-style-type: none"> CA selects the HSM Output terminal window. Utilize the HSM's keyboard to scroll through the menu using < > Select "7.Role Mgmt", press ENT to confirm. When "Insert Card SO #X?" is displayed, insert the SO card. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the SO card. Repeat steps d) to f) for the 2nd and 3rd SO card. Select "4.Clear RoleCard", press ENT to confirm. When "Clear Card?" is displayed, press ENT to confirm. When "Num Cards?" is displayed, enter "3", then press ENT. When "Insert Card #X?" is displayed, take the required card and place it on top of the HSM for audit camera display. insert the card into the HSM's card reader. When "Are you sure?" is displayed, press ENT to confirm. <p>Note: The message will differ depending of the card type.</p> <ol style="list-style-type: none"> When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the card. Repeat steps k) to o) until the specified cards have been cleared. Press CLR to return to the main menu "Secured". <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2</p> <p>1st SO card ____ of 7</p> <p>2nd SO card ____ of 7</p> <p>3rd SO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		
4.2	<p>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.</p>		

Act 5: Issue Temporary Adapter Authorization Key (AAK) Cards

When a ceremony includes the introduction of a new HSM, it is necessary to generate temporary AAK cards to allow existing Crypto Officer credentials to perform signing and administrative operations in a new HSM. These temporary cards will be used and subsequently destroyed before the completion of the ceremony.

Note: For a summary of card roles and their purpose see Appendix A number [14].

Issue Temporary Adapter Authorization Key (AAK) Cards

Step	Activity	Initials	Time
5.1	<p>CA performs the following steps to issue temporary Adapter Authorization Key (AAK) cards:</p> <ul style="list-style-type: none"> 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 "3.Backup AAK", press ENT to confirm. i) When "Backup AAK?" is displayed, press ENT to confirm. j) When "Num Cards?" is displayed, enter "2", then press ENT. k) When "Insert Card #X?" is displayed, insert the required AAK card. l) When "Remove Card?" is displayed, remove the AAK card. m) Repeat steps k) to l) for the 2nd AAK card. n) When "Done AAK" is displayed, press ENT to confirm. o) Press CLR to return to the menu "Secured". <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2</p> <p>1st SO card ____ of 7</p> <p>2nd SO card ____ of 7</p> <p>3rd SO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
5.2	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.		
5.3	CA performs the following steps to prepare the HSM for storage: <ul style="list-style-type: none"> a) Ask the IW for the HSM's designated new TEB, and read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB and seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. HSM6W: TEB # BB51184550 / Serial # H2008009		

Act 6: Introduce New HSM

Keyper HSMs are replaced approximately every four to five years to better ensure reliable operation of the Root Zone KSK function. Pursuant to these procedures, new HSMs are periodically introduced.

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 a secure state
- Change and verify API settings
- Import Storage Master Key (SMK)
- Import App Key (KSK)
- Verify connectivity, activate, and initialize HSM
- Destroy temporary AAK cards

HSM8W (Tier 7) Setup

Step	Activity	Initials	Time
6.1	<p>CA performs the following steps to prepare the HSM:</p> <ol style="list-style-type: none"> Remove the TEB from the cart and place it on the ceremony table. Inspect the TEB for tamper evidence. Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. <p>HSM8W: TEB # BB51184549 / Serial # H2110006 Last Verified: AT Ceremony 52 2024-02-13</p> <p>Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		

Power ON the HSM8W (Tier 7)

Step	Activity	Initials	Time
6.2	CA selects the HSM Output terminal window.		
6.3	<p>CA performs the following steps to prepare the HSM:</p> <ol style="list-style-type: none"> Verify the label on the HSM reads HSM8W. Plug the null modem cable into the serial port of the HSM. Connect the power to the HSM, then switch it ON. Note: Status information should appear in the HSM output terminal window. Scroll up on the terminal window while IW verifies the displayed HSM serial number on the screen reads H2110006. Scroll down to the end of the terminal window. After the completion of the HSM self test the display should say "Important Read Manual" indicating the HSM is in the initialized state. <p>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</p>		

Import the AAK

Step	Activity	Initials	Time
6.4	<p>CA performs the following steps to import the Adapter Authorization Key (AAK):</p> <ol style="list-style-type: none"> 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. <p>Each card is returned to its designated card holder after use.</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Configure the HSM to Secure State

Step	Activity	Initials	Time
6.5	<p>CA performs the following steps to configure the HSM to secure state:</p> <ul style="list-style-type: none"> 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. <p>Done Rebooting Device will be displayed.</p> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Change the API Settings

Step	Activity	Initials	Time
6.6	<p>CA performs the following steps to change the API settings:</p> <ul style="list-style-type: none"> 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. 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". <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2</p> <p>1st CO card ____ of 7</p> <p>2nd CO card ____ of 7</p> <p>3rd CO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Verify API Settings

Step	Activity	Initials	Time
6.7	<p>CA performs the following steps to dump the status of the HSM:</p> <ul style="list-style-type: none"> 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". f) 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. g) After verification, scroll down to the end of the terminal window. <pre> 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 </pre>		

App Key Backups

Step	Activity	Initials	Time
6.8	<p>CA performs the following steps to prepare the App key backups:</p> <ul style="list-style-type: none"> 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 App key cards and the backup HSMFD on its designated area of the ceremony table. e) If not already present, place corresponding labels on the APP key plastic case and ensure their respective HSMFDs remain in the plastic case. <p>KSK-2017: TEB # BB02638568 Last Verified: KSK Ceremony 48 2023-02-01 KSK-2023: TEB # BB02638507 Last Verified: KSK Ceremony 50 2023-07-19</p> <p>Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		

Import the SMK and the KSK

Step	Activity	Initials	Time
6.9	<p>CA performs the following steps to access the Key Management menu:</p> <ul style="list-style-type: none"> 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. <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2</p> <p>1st CO card ____ of 7</p> <p>2nd CO card ____ of 7</p> <p>3rd CO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Step	Activity	Initials	Time
<p>6.10</p>	<p>CA performs the following steps to import the SMK:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "4.SMK" from the current "Key Mgmt" menu, press ENT to confirm. c) Select "3.Restore SMK", press ENT to confirm. d) When "Restore SMK?" is displayed, press ENT to confirm. e) When "Insert Card SMK #X?" is displayed, insert the SMK card. f) When "Remove Card?" is displayed, remove the SMK card. g) Repeat steps e) to f) for the 2nd and 3rd SMK card. h) When "SMK Restored" is displayed, press ENT to confirm. i) Press CLR once to return to the menu "Key Mgmt". <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2</p> <p>1st SMK card ____ of 7</p> <p>2nd SMK card ____ of 7</p> <p>3rd SMK card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		
<p>6.11</p>	<p>CA performs the following steps to import KSK:</p> <ul style="list-style-type: none"> 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) Repeat steps c) to h) for any remaining App Key card listed below. j) Press CLR twice to return to the main menu "Secured". <p>CA uses the card listed below. Card is returned to its designated card holder after use.</p> <p>KSK-2017: Klajeyz App Key card # 2</p> <p>KSK-2023: Kmrfl3b App Key card # 2</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
6.12	<p>CA performs the following steps to activate the HSM:</p> <ul style="list-style-type: none"> 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. <p>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</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
6.13	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		
6.14	<p>CA performs the following steps to test the network connectivity between laptop and HSM:</p> <ul style="list-style-type: none"> a) Select the Commands terminal window b) Test connectivity by executing: <code>ping hsm</code> c) Wait for responses, then exit by pressing: <code>Ctrl + C</code> 		

Execute the KSR Signer for KSR 2024 Q2

Step	Activity	Initials	Time
6.15	Using the Commands terminal window, the CA executes the command below to change the directory: <code>cd HSM8W/</code>		
6.16	Using the Commands terminal window, the CA executes the command below to sign the KSR file: <code>kskm-ksrsigner</code>		

Verify the KSR Hash for KSR 2024 Q2

Step	Activity	Initials	Time
6.17	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.		
6.18	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks "are there any objections?"		
6.19	CA enters Yes in response to "Sign KSR?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSRFD/KSK52/HSM8W/HSM8W-skr-root-2024-q2-0.xml</code>		

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
6.20	Using the Commands terminal window, the CA executes the commands below to print the KSR Signer log: a) <code>printlog kskm-ksrsigner-202402*.log X</code> Note: Replace "X" with the amount of copies needed for the participants.		
6.21	IW attaches a copy of the required ksr signer log to their script.		

SKR Comparison

Step	Activity	Initials	Time
6.22	CA executes the command below to display the xsl style sheet content: <code>cat style.xml</code>		
6.23	Using the Commands terminal window, the CA executes the commands below to compare the SKRs: a) <code>xsltproc style.xml ../skr-root-2024-q2-0.xml xmllint --format - > current</code> b) <code>xsltproc style.xml HSM8W-skr-root-2024-q2-0.xml xmllint --format - > new</code> c) <code>diff -wu current new</code> Note: When executing a diff command, a return of no output indicates a match.		
6.24	Using the Commands terminal window, the CA executes the command below to change the directory: <code>cd /media/HSMFD</code>		

Copy the Newly Generated SKR

Step	Activity	Initials	Time
6.25	<p>CA executes the following commands using the terminal window:</p> <ul style="list-style-type: none"> a) List the contents of the KSRFD by executing: <code>ls -ltrR /media/KSRFD</code> b) Copy the contents of the KSRFD to the HSMFD by executing: <code>cp -pR /media/KSRFD/* .</code> <p>Note: Confirm overwrite by entering "y" if prompted.</p> <ul style="list-style-type: none"> c) List the contents of the HSMFD by executing: <code>ls -ltrR</code> d) Verify it has been copied successfully by executing: <code>diff -qr /media/HSMFD/KSK52/ /media/KSRFD/KSK52/</code> e) Unmount the KSRFD by executing: <code>umount /media/KSRFD</code> <p>Note: When executing a diff command, a return of no output indicates a match.</p>		
6.26	<p>CA removes the KSRFD containing the SKR files, then gives it to the RZM representative.</p> <p>Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.</p>		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
6.27	<p>CA deactivates the HSM by performing the following steps:</p> <p>Note: CA will use OP cards not previously utilized in this ceremony if available.</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>Set # 2</p> <p>1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		

Clear and Destroy AAK Cards

Step	Activity	Initials	Time
6.28	<p>CA performs the following steps to clear Adapter Authorization Key (AAK) cards:</p> <ul style="list-style-type: none"> 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 d) to f) for the 2nd and 3rd SO card. g) Select "5.Clear AAK Card", press ENT to confirm. h) When "Clear AAK Card?" is displayed, press ENT to confirm. i) When "Num Cards?" is displayed, enter "2", then press ENT. j) 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. k) When "Are you sure?" is displayed, press ENT to confirm. l) When "Remove Card?" is displayed, remove the AAK card. m) Repeat steps j) to l) for the 2nd AAK card. n) Press CLR to return to the main menu "Secured". <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 2 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix A number [14].</p>		
6.29	<p>CA uses the shredder to destroy the cleared AAK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.</p>		

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
6.30	<p>CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.</p> <p>Note: DO NOT unplug the cable connections on the laptop.</p>		
6.31	<p>CA performs the following steps to prepare the HSM for storage:</p> <ul style="list-style-type: none"> a) Ask the IW for the HSM's designated new TEB, and read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB and seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. <p>HSM8W: TEB # BB51184551 / Serial # H2110006</p>		

Return the KSK into a TEB

Step	Activity	Initials	Time
6.32	<p>CA performs the following steps to prepare the KSK for storage:</p> <ul style="list-style-type: none"> a) Ask the IW for the KSK's designated new TEB, and read the TEB number aloud while IW verifies it matches the information below. b) Place the KSK into its plastic case along with the backup HSMFD c) Place the plastic case into its designated new TEB and seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the KSK onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the KSK TEB on the cart. <p>KSK-2017: TEB # BB02638483 KSK-2023: TEB # BB02638484</p>		

Act 7: Secure Hardware

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

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

Stop Logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
7.1	<p>CA performs the following steps to stop logging:</p> <p>a) Perform the following steps using the HSM Output terminal window to stop logging the serial output (ttyaudit):</p> <p>i) Press Ctrl + C</p> <p>ii) Execute exit</p> <p>b) Execute the command below using the Commands terminal window to stop logging the terminal session:</p> <p>exit</p> <p>Note: The Commands terminal session window will remain open.</p> <p>c) Disconnect the null modem and ethernet cables from the laptop.</p>		

Print Logging Information

Step	Activity	Initials	Time
7.2	<p>CA executes the following commands to print a copy of the logging information:</p> <p>a) <code>print-script script-202402*.log</code></p> <p>b) <code>print-ttyaudit ttyaudit-tty*-202402*.log</code></p> <p>Attach the printed copies to IW script.</p> <p>Note: Ignore the error regarding non-printable characters if prompted.</p>		

Prepare Blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
7.3	<p>CA executes the following command to print two copies of the hash for the HSMFD content:</p> <p><code>hsmfd-hash -p</code></p> <p>Note: One copy for the audit bundle and one copy for the OS Media TEB.</p>		
7.4	<p>CA executes the command below to display the contents of the HSMFD:</p> <p><code>ls -ltrR</code></p>		
7.5	<p>CA executes the command below to set the <code>copy-hsmfd</code> script to verbose mode:</p> <p><code>sed -i '4i set -x' /opt/icann/bin/copy-hsmfd</code></p>		
7.6	<p>CA executes the command below and follows the interactive prompts in the terminal window to create five HSMFDs copies:</p> <p><code>copy-hsmfd</code></p> <p>Note: Wait for the activity light on the copied HSMFD to stop flashing before removal.</p>		

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
7.7	<p>CA executes the following commands using the terminal window to unmount the HSMFD:</p> <ul style="list-style-type: none"> a) <code>cd /tmp</code> b) <code>umount /media/HSMFD</code> <p>CA removes the HSMFD, then places it on the holder.</p> <p>Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.</p>		
7.8	<p>CA performs the following steps to shut down the laptop:</p> <ul style="list-style-type: none"> 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. d) Close all laptop latches. 		
7.9	<p>CA performs the following steps to prepare the OS Media Bundle for storage:</p> <ul style="list-style-type: none"> a) Ask the IW for the OS Media Bundle's designated new TEB, and read the TEB number aloud while IW verifies it matches the information below. b) Place 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 seal it. c) Give IW the sealing strips for post-ceremony inventory. d) Place the OS Media Bundle onto the HSM designated space of the ceremony table visible to the audit camera. e) Initial the TEB along with IW using a ballpoint pen. f) Place the OS Media Bundle TEB on the cart. <p>OS media (release coen-1.0.0) + HSMFD: TEB # BB02638482</p>		
7.10	<p>CA distributes the following HSMFDs:</p> <ul style="list-style-type: none"> 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
7.11	<p>CA performs the following steps to prepare the Laptop for storage:</p> <ul style="list-style-type: none"> a) Ask the IW for the Laptop's designated new TEB, and read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the service tag number from the bottom of the laptop while the IW verifies it matches the information below. c) Place the Laptop into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the Laptop onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the Laptop TEB on the cart. <p>Laptop3: TEB # BB97448417 / Service Tag # C8SVSG2</p>		

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
7.12	<p>The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps:</p> <ul style="list-style-type: none"> a) CA asks the IW for the CO's designated new TEB, and reads the TEB number and description aloud while IW verifies it matches the information below. b) CO removes their credentials from the card holder and places them inside an available 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, then seals it. e) CA gives the IW sealing strips for post-ceremony inventory. f) CA initials the TEB with a ballpoint pen. g) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. h) CA gives the TEB containing the cards to the CO. i) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. j) CO writes the date and time, signs the credential table of the IW's script, then the IW initials the entry. k) CO returns to their seat with their TEBs, being especially careful not to compromise any TEB. l) Repeat steps for all the remaining COs' credentials on the list. <p>CO1: Arbogast Fabian Set # 2 TEB # BB02638485</p> <p>CO2: Ralf Weber Set # 2 TEB # BB02638486</p> <p>CO5: Ólafur Guðmundsson Set # 2 TEB # BB02638487</p> <p>CO6: Jorge Etges Set # 2 TEB # BB02638488</p>		

CO	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	Set # 2 TEB # BB02638485	Arbogast Fabian		2024 Feb __		
CO2	Set # 2 TEB # BB02638486	Ralf Weber		2024 Feb __		
CO5	Set # 2 TEB # BB02638487	Ólafur Guðmundsson		2024 Feb __		
CO6	Set # 2 TEB # BB02638488	Jorge Etges		2024 Feb __		

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

Note: The shelves in the equipment safe can slide in and out for ease of use.

Step	Activity	Initials	Time
7.13	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
7.14	SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.		
7.15	SSC1 removes the safe log, writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		
7.16	CA performs the following steps to return each piece of equipment to the safe: <ol style="list-style-type: none"> CAREFULLY remove the equipment TEB from the cart. Read aloud the TEB number, verify its integrity. Present the equipment TEB to the audit camera above, then place it inside Safe #1. Write the date, time, and signature on the safe log where "Return" is indicated. IW verifies the safe log entry, then initials it. <p>HSM6W: TEB # BB51184550 HSM8W: TEB # BB51184551 Laptop3: TEB # BB97448417 OS media (release coen-1.0.0) + HSMFD: TEB # BB02638482 KSK-2017: TEB # BB02638483 KSK-2023: TEB # BB02638484</p> Note: The shelves in the equipment safe can slide in and out for ease of use.		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
7.17	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the entry, then initials it.		
7.18	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 adjacent to the Tier 5 (Safe Room) exit door is off.		
7.19	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
7.20	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)		
7.21	SSC2 opens Safe #2 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.		
7.22	SSC2 removes the safe log, writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		

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

Step	Activity	Initials	Time
	<p>COs perform the following steps sequentially to return the listed TEBs:</p> <ul style="list-style-type: none"> a) CO reads aloud the TEB number, verifies integrity of TEB, then presents it to the audit camera above. b) After the CA operates the guard key in the lower lock, CO reads aloud the safe deposit box number and uses their tenant key to operate the upper lock. 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. f) CA locks the safe deposit box and removes the guard key. 		
7.23	<p>CO1: Arbogast Fabian Box # 1788 Set # 2 TEB # BB02638485</p> <p>CO2: Ralf Weber Box # 1071 Set # 2 TEB # BB02638486</p> <p>CO5: Ólafur Guðmundsson Box # 1070 Set # 2 TEB # BB02638487</p> <p>CO6: Jorge Etges Box # 1072 Set # 2 TEB # BB02638488</p>		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
7.24	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the safe log entry, then initials it.		
7.25	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 adjacent to the Tier 5 (Safe Room) exit door is off.		
7.26	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).		

Act 8: Close the Key Signing Ceremony

The CA will finish the ceremony by performing the following steps:

- Read any exceptions that occurred during the ceremony
- Call the ceremony participants to sign the IW's script
- Stop the online streaming and video recording

Participants Sign IW's Script

Step	Activity	Initials	Time
8.1	CA reads all exceptions that occurred during the ceremony.		
8.2	CA calls each in-person attendee not seated at the ceremony table to sign the IW's participant list. All signatories declare to the best of their knowledge that this script is a true and accurate record of the ceremony.		
8.3	CA reviews IW's script, then signs the participants list.		
8.4	IW signs the list and records the completion time.		

Stop Online Streaming and Recording

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

Appendix A: Glossary

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

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

- [2] **configure-printer**:* A bash script used to install the HP LaserJet print driver from the command line instead of **system-config-printer**.
- [3] **copy-hsmfd**:* A bash script used to copy HSMFD contents to new flash drives; includes verification via hash comparison.
- [4] **hsmfd-hash**:* A bash script used to calculate, print, and compare SHA-256 checksums for the HSMFD flash drives.
Note: The sort command has different behavior depending on the locale settings specified by environment variables. Current OS locale setting is LC_COLLATE="POSIX"
- [5] **kskm-keymaster**:** An application that creates and deletes keys and performs a key inventory.
- [6] **kskm-ksrsigner**:** An application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.
- [7] **ksrsigner**: A legacy application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.

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

- [8] **ping hsm**: The HSM static IP address `192.168.0.2` has been included in the `/etc/hosts` file.
- [9] **printlog**:* A bash script used to print the Key Signing Log output from **ksrsigner** application.
- [10] **print-script**:* A bash script used to print the terminal commands.
- [11] **print-ttyaudit**:* A bash script used to print the HSM logs.
- [12] **sha2wordlist**: An application that reads data from STDIN and outputs a SHA-256 checksum as hex and PGP words in STDOUT.

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

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

* The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-1.0.0coen_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>

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

- a) **OP (Operator)**: Configures the HSM to an online or offline state toggling communication through its ethernet adapter. Required for communication with the laptop for key signing operations.
- b) **SO (Security Officer)**: Used for HSM administrative operations. Required to create other role cards (OP and CO), and the introduction or zeroization of an HSM.
- c) **CO (Crypto Officer)**: Used for the key management functions in an HSM. Required for adding or deleting keys stored in an HSM.
- d) **SMK (Storage Master Key)**: Allows an HSM to read an encrypted APP key backup. Required for initial migration of keys and disaster recovery.
- e) **AAK (Adapter Authorization Key)**: Configures an HSM to use previously generated OP, CO, and SO cards. Required for the introduction of an HSM.
- f) **APP (Application Key)**: An encrypted backup copy of one or more keys stored in an HSM, which can only be decoded by its corresponding SMK. Required for migrating keys and disaster recovery.

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

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

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

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

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

Two electronic copies of the following:

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

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

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

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

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

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

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

7. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 52**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

Appendix C: Key Ceremony Script (by IW)

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

IW: **Jonathan Denison**

Signature:

Date: 2024 Feb __

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: **20230719 00:00:00 to 20240215 00:00:00 UTC.**

SA:

Signature:

Date: 2024 Feb __

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: 2024 Feb __