Root DNSSEC KSK Ceremony 40

Wednesday February 12, 2020

Root Zone KSK Operator Key Management Facility
1920 East Maple Avenue, El Segundo, CA 90245

This ceremony is executed in accordance to the DNSSEC Practice Statement for the Root Zone KSK Operator Version 4th Edition (2016-10-01)

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	Gustavo Lozano / ICANN		2020 Feb —	
IW	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Hilary Jin / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO3	João Damas			
CO4	Carlos Martinez			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Trevor Davis / Verisign			
RZM	Duane Wessels / Verisign			
RZM	Chris Browning / Verisign			
AUD	Karen Minh Phan / RSM			
AUD	Eylan Jordan Torres / RSM			
SA	Brian Martin / ICANN			
SA	Patrick Tudor / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Gina Villavicencio / ICANN			
SW	Göran Marby / ICANN			
EW	George Palmer			
EW	Alex Boyd			
EW	Mimi Rauschendorf			

Note: 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 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 CAs, IWs, or SAs 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
- CAs, IWs, or SAs may escort participants out of Tier 4 (Key Ceremony Room) at the CA's discretion only if Tier 5 (Safe Room) is not occupied during the ceremony
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log
- The SA starts filming before the participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step
- CA reads each step aloud prior to its performance
- Upon completion of each step, IW announces the time of completion, records the completion time, and initials their copy of the script
- Ceremony participants who notice a problem or an error during the ceremony should interrupt the ceremony. Ceremony participants agree on a resolution before proceeding
- 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 tell and/or confirm identifiers comprised of numbers and letters. When spelling identifiers, the phonetic alphabet shown below must 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

At this point, the CA and IW will escort the SSCs and TCRs into Tier 5 (Safe Room) to retrieve the following materials:

- Safe #1: HSM, laptop, OS DVD, etc
- Safe #2: The TCRs' 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 introduce themselves.		

Emergency Evacuation Procedures and Electronics Policy

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

Verify the Time and Date

Step	Activity	Initials	Time
7	IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time:_____ All entries into this script or any logs should follow this common source of time.		

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
8	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)		
9	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.**		
10	Perform the following steps to complete the safe log: a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.		

COs Extract the Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
11	COs perform the following steps sequentially to retrieve the required TEBs: a) With the assistance of the CA (and the common key), the CO opens their safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock.** 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. **Note: The CO's key will remain inserted in their safe deposit box lock when specified below.** e) CO writes the date and time, then signs the safe log where removal of a TEB is indicated. f) IW verifies the completed safe log entries, then initials it. **CO1: Arbogast Fabian** **Box # 1791 (Key shall remain in lock)** **OP TEB # BB46584376 (Retain)** **SO TEB # BB46584377 (Retain)** **CO2: Dmitry Burkov** **Box # 1793 (Key shall remain in lock)** **OP TEB # BB46584378 (Retain)** **SO TEB # BB46584379 (Retain)** **CO3: João Damas** **Box # 1071 (Key shall remain in lock)** **OP TEB # BB46592091 (Retain)** **SO TEB # BB46584455 (Retain)** **CO4: Carlos Martinez** **Box # 1068 (Key shall remain in lock)** **OP TEB # BB46592092 (Retain)** **SO TEB # BB46584665 (Retain)** **CO6: Nicolas Antoniello** **Box # 1073 (Key shall remain in lock)** **OP TEB # BB46584382 (Retain)** **SO TEB # BB46584383 (Retain)** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46584384 (Retain)** **SO TEB # BB46584385 (Retain)**		

Close Safe #2 (Tier 6, Credentials Safe)

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

Open Safe #1 (Tier 6, Equipment Safe)

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

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

Step	Activity	Initials	Time
18	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified on 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. **HSM3: TEB # BB51184512 (Place on Cart)** **HSM4: TEB # BB51184513 (Place on Cart)** **HSM5W: TEB # BB51184514 (Check and Return)** **Laptop3: TEB # BB81420125 (Check and Return)** **Laptop4: TEB # BB81420103 (Place on Cart)** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386 (Place on Cart)** **KSK-2017: TEB # BB46584387 (Check and Return)** **HSM3 Physical Keyboard Key: TEB # BB21907221 (Place on Cart)**		

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

Step	Activity	Initials	Time
19	SSC1 writes the date and time, then signs the safe log where Close Safe is indicated. IW verifies the safe log entry then initials it.		
20	SSC1 returns the safe log 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.		
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 DVD (the laptop has no permanent storage device)
- Set up the printer
- Verify 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. **HSM4: TEB # BB51184513 / Serial # H1411006** **Last Verified: KSK38 2019-08-14** **Laptop4: TEB # BB81420103 / Service Tag # F8SVSG2** **Last Verified: KSK36 2019-02-27** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386** **Last Verified: KSK38 2019-08-14**		
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**[1] 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`[2] `< /dev/sr0` IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.** SHA-256 hash: **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/40**		

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`[3]		

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 "20200212 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 38 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`[4] `-c`** IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 38 annotated script. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.** **HSMFD SHA-256 HASH** **2019/08/15** `# find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist` SHA-256: 94862bfae4991cb5b47ed294dab7d5a03c031b0c1f16acb1b61af65ca905bc85 PGP Words: Pluto letterhead briefcase whimsical tonic nebula befriend positive scenic insurgent standard molecule surmount processor sterling Orlando cobra aggregate beeswax article billiard bodyguard ribcage photograph Scotland Bradbury village fascinate revenge almighty showgirl leprosy		

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 38** 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-20200212.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`[5] **`/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) Ensure an RJ45 blockout is present in the "MGMT" port of the HSM. Install one if not present. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** d) Scroll the logging screen up and locate the HSM serial number. e) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. **HSM4: Serial # H1411006** **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 TCRs' 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
- Note: The SKR contains the digital signatures of the ZSK slated to be used in the next quarter
- The CA then prints the signer log, backs up the newly created SKR, and deactivates the HSM

TCR 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. **CO1: Arbogast Fabian** **OP TEB # BB46584376** **SO TEB # BB46584377** **CO2: Dmitry Burkov** **OP TEB # BB46584378** **SO TEB # BB46584379** **CO3: João Damas** **OP TEB # BB46592091** **SO TEB # BB46584455** **CO4: Carlos Martinez** **OP TEB # BB46592092** **SO TEB # BB46584665** **CO6: Nicolas Antoniello** **OP TEB # BB46584382** **SO TEB # BB46584383** **CO7: Subramanian Moonesamy** **OP TEB # BB46584384** **SO TEB # BB46584385**		

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`[6] c) Wait for responses, then exit by pressing: `Ctrl + C`		

Insert the KSR FD

Step	Activity	Initials	Time
5	CA plugs the FD labeled **"KSR"** then waits for it to be recognized by the OS. CA points out the KSR file that will be signed on each folder, then closes the file system window. **Note: The KSR FD was transferred to the facility by the RKOS. It contains 1 KSR.**		

Execute the KSR Signer for KSR 2020 Q2

Step	Activity	Initials	Time
6	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[7] `/media/KSR/KSK40/ksr-root-2020-q2-0.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 2020 Q2

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed on the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themself in front of the room and provide documents for IW to review off camera for the purpose of authentication. b) IW retains the hash and PGP word list for KSR 2020 Q2, and employment verification letter provided by the RZM representative and writes their name on the following line: _____ 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 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/KSK40/skr-root-2020-q2-0.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`**[8] **`ksrsigner-202002*.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 KSR FD by executing: **`ls –ltrR /media/KSR`** b) Copy the contents of the KSR FD 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 KSR FD by executing: **`umount /media/KSR`**		
14	CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative.		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
15	CA utilizes the unused OP cards to deactivate the HSM: 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.**		

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
16	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.**		
17	CA places the HSM into a prepared TEB, then seals it.		
18	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. **HSM4: TEB # BB51184227 / Serial # H1411006**		

Act 4: Zeroize and Dismantle Hardware Security Module

To conclude its period of service, the retiring HSM will be zeroized and have its critical components removed and securely destroyed.

- CA will generate temporary CO cards
- CA will remove all keys from the HSM
- CA will destroy temporary CO cards
- CA will zeroize the HSM
- CA will intentionally tamper the HSM
- CA will dismantle the HSM and extract its critical components
- CA will place the components into a TEB in preparation for offsite secure destruction

Remove the HSM from TEB and Power On

Step	Activity	Initials	Time
1	CA selects the **HSM Output** terminal window.		
2	CA performs the following steps to prepare the HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. 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. **HSM3: TEB # BB51184512 / Serial # H1403033** **Last Verified: KSK38 2019-08-14** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Issue Temporary Crypto Officer (CO) Cards

Step	Activity	Initials	Time
3	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are used 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** twice to return to the **"Secured"** menu. 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.**		

List and Delete the KSK(s) present in the HSM

Step	Activity	Initials	Time
4	CA performs the following steps to list the KSK(s) present in the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert 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 **"2.Key Details"**, press **ENT** to confirm. h) When **"List Keys?"** is displayed, press **ENT**. i) Select **"1.Key Summary"**, press **ENT** to confirm. j) When **"Key Summary?"** is displayed, press **ENT**. 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.**		
5	CA matches the displayed KSK label(s) in the HSM Output terminal window. **KSK-2017: Klajeyz**		
6	CA performs the following steps to delete the KSK(s) from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"7.Erase App Key"**, press **ENT** to confirm. d) When **"Erase App Keys?"** is displayed, press **ENT** to confirm. e) Select **"1.All Keys"**, press **ENT** to confirm. f) The **Klajeyz** key(s) will be selected in the HSM's display with a visible (*) asterisk. Press **ENT** to confirm. **There is no system confirmation prompt**. g) When **Done** is displayed, press **ENT** to return to the App Key Menu. h) Press **CLR** to return to the Key Mgmt menu.		
7	CA performs the following steps to list the KSK(s) from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. f) Press **CLR** to return to the menu **"Secured"**. CA confirms that **KSK-2017: Klajeyz** has been deleted		

Clear and Destroy CO Cards

Step	Activity	Initials	Time
8	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 **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. l) When **"Remove Card?"** is displayed, remove the CO card. m) Repeat steps j) to l) for the 2nd CO card. n) Press **CLR** to return to the main menu **"Secured"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # ____ 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.**		
9	CA uses the shredder to destroy the cleared CO cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.		

Unsecure and Tamper the HSM

Step	Activity	Initials	Time
10	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 **"6.HSM 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 **"5.Unsecure"**, press **ENT** to confirm. h) When **"Unsecure?"** is displayed, then press **ENT**. i) When **"DONE"** is displayed, then press **ENT**. It may take a few minutes for the HSM to restart after the zeroization is complete. The HSM will reboot into the **"Unsecured State"** and after the completion of the HSM self test the display should show **"Important Read Manual"** indicating the HSM is in the initialized state. 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.**		
11	CA performs the following steps to tamper the HSM equipment listed below: a) Using **Tool B**, press and hold the recessed button on the rear panel of the HSM located between the LAN and serial ports (remove the tamper sticker if necessary), then release it after 10 seconds to activate the tampering mechanism. **IMK missing recovery mode** will be displayed on the HSM. b) Turn **OFF** the HSM using the rocker switch on the rear panel. Turn **ON** the HSM with the same switch and wait until the **ALERT** LED light is **ON** and **IMK missing recovery mode** is displayed to verify the tampered state. c) Disconnect the power and serial cables from the HSM.		

Open the HSM Case and Remove the Logic Board from HSM3

Step	Activity	Initials	Time
12	IW reads steps 13 to 16 while the CA dismantles **HSM3: Serial # H1403033**.		
13	CA performs the following steps to access the HSM's critical components: a) Using **Tool A+Bit 2**, remove the two screws which secure the serial port to the rear panel. b) Using **Tool A+Bit 1**, remove the four screws from the rear panel of the case which secure the shell. c) Using **Tool A+Bit 1**, remove the four screws from the bottom of the case which secure the shell. d) Using **Tool C**, slice the tamper stickers on the bottom of the case along the seam with the shell. e) Slide the shell toward the back of the case to remove it and place it in the **HSM Parts** bin on the ceremony table. f) Using **Tool A+Bit 3**, remove the two logic board screws nearest to the front panel which secure the plastic logic board cover. g) Remove the plastic logic board cover and place it in the **HSM Parts** bin on the ceremony table. h) Using **Tool A+Bit 3**, remove the two remaining screws which secure the logic board near the rear panel. i) Detach the four cables from the front of the logic board. Open the latches outward to release each of the ribbon cables. j) Using **Tool A+Bit 4**, remove the nut from the cryptographic module securing the ring terminal of the green/yellow wire and slide the ring terminal off of the threaded stud. k) Detach the cable from each side of the cryptographic module connecting it to the logic board.		
14	CA performs the following steps to remove the logic board and batteries: a) Separate the logic board from the HSM case by pulling the logic board up then toward the front of the case. b) Using **Tool D**, cut and remove the zip ties securing the batteries if they are present, then cut the battery terminals that connect the batteries to the logic board. c) Pry the batteries from the logic board by placing the logic board flat on the table and pulling up on each battery with sufficient force to break the adhesive bond. d) Place the batteries in the **HSM Parts** bin on the ceremony table. e) Place the logic board in the **Critical Parts** bin on the ceremony table.		

Remove Cryptographic Module and Card Reader from HSM3

Step	Activity	Initials	Time
15	CA performs the following steps to remove the cryptographic module: a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the cryptographic module to the case. b) Lift the cryptographic module up to separate it from the case. c) Using **Tool C**, remove both connectors from the cryptographic module as flush with the case as possible. d) Place the cryptographic module in the **Critical Parts** bin, and the connectors in the **HSM Parts** bin on the ceremony table.		
16	CA performs the following steps to remove the front panel and card reader: a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the front panel to the bottom of the case. b) Place the front panel in the **HSM Parts** bin on the ceremony table. c) Using **Tool A+Bit 4**, remove the nut which secures the card reader. d) Using **Tool A+Bit 3**, remove the 3 screws which secure the card reader. e) Lift the card reader up to separate it from the case and place it with the ribbon cable in the **Critical Parts** bin on the ceremony table. f) Place the HSM case in the **HSM Parts** bin on the ceremony table.		

Place the Critical HSM3 parts into a TEB

Step	Activity	Initials	Time
17	CA places the container with the following critical parts into a prepared TEB, then seals it. a) Cryptographic Module b) Logic Board c) Card Reader **Note: The HSM case will not be destroyed.**		
18	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) Give RKOS the TEB for destruction. **HSM3: TEB # BB81420112**		

Retire HSM Physical Keyboard Key

Step	Activity	Initials	Time
19	CA performs the following steps to retire the listed HSM Physical Keyboard Key: a) Remove the TEB from the cart. b) Inspect 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. e) RKOS will take possession of the HSM Physical Keyboard Key and place in its designated area. **HSM3 Physical Keyboard Key: TEB # BB21907221** **Last Verified: AT22 2015-07-20**		

Act 5: 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 TCR 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 TCRs into Tier 5 (Safe Room) to return TCRs' 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[4] –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[4] -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-202002*.log`** c) **`enscript -Gr --font="Courier8" ttyaudit-tty*-202002*.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 including power, printer, and display.		
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 # BB91951332**		

Distribute the HSMFDs

Step	Activity	Initials	Time
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 # BB81420113 / Service Tag # F8SVSG2**		

Place HSM Cards 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 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. **CO1: Arbogast Fabian** **OP TEB # BB91951344** **SO TEB # BB91951343** **CO2: Dmitry Burkov** **OP TEB # BB91951342** **SO TEB # BB91951341** **CO3: João Damas** **OP TEB # BB91951340** **SO TEB # BB91951339** **CO4: Carlos Martinez** **OP TEB # BB91951338** **SO TEB # BB91951337** **CO6: Nicolas Antoniello** **OP TEB # BB91951336** **SO TEB # BB91951335** **CO7: Subramanian Moonesamy** **OP TEB # BB91951334** **SO TEB # BB91951333**		

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	**OP 1 of 7** **SO 1 of 7**	OP TEB # **BB91951344** SO TEB # **BB91951343**	**Arbogast Fabian**		**2020 Feb __**		
CO2	**OP 2 of 7** **SO 2 of 7**	OP TEB # **BB91951342** SO TEB # **BB91951341**	**Dmitry Burkov**		**2020 Feb __**		
CO3	**OP 3 of 7** **SO 3 of 7**	OP TEB # **BB91951340** SO TEB # **BB91951339**	**João Damas**		**2020 Feb __**		
CO4	**OP 4 of 7** **SO 4 of 7**	OP TEB # **BB91951338** SO TEB # **BB91951337**	**Carlos Martinez**		**2020 Feb __**		
CO6	**OP 6 of 7** **SO 6 of 7**	OP TEB # **BB91951336** SO TEB # **BB91951335**	**Nicolas Antoniello**		**2020 Feb __**		
CO7	**OP 7 of 7** **SO 7 of 7**	OP TEB # **BB91951334** SO TEB # **BB91951333**	**Subramanian Moonesamy**		**2020 Feb __**		

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 will begin by rapidly spinning the dial counter-clockwise in order to charge it.**		
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. **HSM4: TEB # BB51184227** **Laptop4: TEB # BB81420113** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951332**		

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 will begin by rapidly spinning the dial counter-clockwise in order to charge it.**		
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) With the assistance of the CA (and the common key), the CO opens their safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock.** c) CO reads aloud the safe deposit box number, places their TEB(s) inside, then locks the safe deposit box. **Note: The COs will retrieve their new safe deposit box keys when specified below.** d) CO writes the date and time, then signs the safe log where **"Return"** is indicated. e) IW verifies the completed safe log entry, then initials it. **CO1: Arbogast Fabian** **Box # 1788 (Retrieve keys from lock)** **OP TEB # BB91951344** **SO TEB # BB91951343** **CO2: Dmitry Burkov** **Box # 1790 (Retrieve keys from lock)** **OP TEB # BB91951342** **SO TEB # BB91951341** **CO3: João Damas** **Box # 1069 (Retrieve keys from lock)** **OP TEB # BB91951340** **SO TEB # BB91951339** **CO4: Carlos Martinez** **Box # 1070 (Retrieve keys from lock)** **OP TEB # BB91951338** **SO TEB # BB91951337** **CO6: Nicolas Antoniello** **Box # 1072 (Retrieve keys from lock)** **OP TEB # BB91951336** **SO TEB # BB91951335** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB91951334** **SO TEB # BB91951333**		

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 6: Close the Key Signing Ceremony

The CA will finish the ceremony by:

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

Participants Signing of 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 signatures 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 once all other participants have signed.		

Stop Online Streaming

Step	Activity	Initials	Time
5	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.		

Post Ceremony Information

Step	Activity	Initials	Time
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 Video 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. Each Audit bundle contains: 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: **20190814 00:00:00 to 20200213 00:00:00 UTC** e) IW's attestation (Appendix C). f) SA's attestation (Appendix D and E). All TEBs are labeled **Root DNSSEC KSK Ceremony 40**, 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-255 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[2]
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*

---

* 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.

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

Two sets of the audit camera footages - 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.

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. 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 to this script.
Any exceptions that occurred were accurately and properly documented.

IW: **Yuko Green**

Signature: _____

Date: 2020 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 on 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: **20190814 00:00:00 to 20200213 00:00:00 UTC.**

SA: _____

Signature: _____

Date: 2020 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 4th Edition (2016-10-01). There are no part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA:

_____

Signature:

_____

Date: 2020 Feb __