Root DNSSEC KSK Ceremony 36

Wednesday February 27, 2019

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		2019 Feb —	
IW	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO3	Joao Damas			
CO4	Carlos Martinez			
CO5	Olafur Gudmundsson			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Duane Wessels / Verisign			
RZM	Brad Verd / Verisign			
RZM	Trevor Davis / Verisign			
AUD	Christopher Koucheki / RSM			
AUD	Catherine Chih-Yun Won / RSM			
SA	Brian Martin / ICANN			
SA	Josh Jenkins / ICANN			
IW2 Backup	David Prangnell / PTI			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW3 Backup	Aaron Foley / PTI			
SW	Mauro Lozano / ICANN			
SW	Dacoda Strack / ICANN			
EW	Collins Takamoto			
EW	James Proud			
EW	Frank Gibson			

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.

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 the 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 the Safe room is not occupied during 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 inside 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 Equipment

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 on Tier 4 (Key Ceremony Room) log
- 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 equipment:

- Safe #1: HSM, laptop, OS DVD, etc
- Safe #2: The TCRs cards required to operate the HSM

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.		
2	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2.		
3	CA asks that any new 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.		
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, time, and signature on 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	The selected CO then performs 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 its integrity while showing it to the audit camera above. d) CO retains the TEB specified below, then locks the safe deposit box. e) CO writes the date, time, and signature on the safe log where removal of TEBs are indicated. f) IW verifies the completed safe log entries, then initials it. **CO1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46592057 (Retain)** **SO TEB # BB46584451 (Check and Return)** **CO2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46592058 (Retain)** **SO TEB # BB46584453 (Check and Return)** **CO3: Joao Damas** **Box # 1071** **OP TEB # BB46592048 (Retain)** **SO TEB # BB46584455 (Check and Return)** **CO4: Carlos Martinez** **Box # 1068** **OP TEB # BB46592050 (Retain)** **SO TEB # BB46584665 (Check and Return)** **CO5: Olafur Gudmundsson** **Box # 1789** **OP TEB # BB46592051 (Retain)** **SO TEB # BB46584666 (Check and Return)** **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46592060 (Retain)** **SO TEB # BB46584459 (Check and Return)** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46592063 (Retain)** **SO TEB # BB46584461 (Check and Return)**		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
12	Once all deposit boxes are closed and locked, SSC2 writes the date, time, and signature on the safe log where "Close Safe" is indicated. IW verifies the entry then initials it.		
13	SSC2 returns the safe log to Safe #2 and locks it 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 the safe room with TEBs, closing the door behind them.		

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.		
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, time, and signature on 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 # BB51184667 / Serial # H1403033 (Check and Return)** **HSM4: TEB # BB51184642 / Serial # H1411006 (Place on Cart)** **Laptop1: TEB # BB51184691 / Serial # 37240147333 (Place on Cart)** **Laptop2: TEB # BB24646591 / Serial # 7292928457 (Place on Cart)** **Laptop3: TEB # BB81420136 / Service Tag # C8SVSG2 (Check and Return)** **Laptop4: TEB # BB81420138 / Service Tag # F8SVSG2 (Place on Cart)** **OS DVD (release 20170403): TEB # BB46592073 (Place on Cart)** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46592066 (Place on Cart)** **Note: The Service Tag # is the same as the Serial Number.**		

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

Step	Activity	Initials	Time
19	SSC1 writes the date, time, and signature on 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 and locks it 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 the safe room with the cart, closing the door behind them.		

Act 2. Equipment Setup

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

- Retire equipment
- Boot the laptop using the OS DVD (the laptop has no permanent storage device)
- Set up the printer
- Verify the laptop date and time
- Format the blank flash drive (HSMFD) that will be used to collect audit evidence
- Connect the HSMFD
- Start the log sessions
- Power ON the HSM (Tier 7)

Retire Equipment

Step	Activity	Initials	Time
1	CA performs the following steps to retire 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.) d) Remove and discard the TEB. e) RKOS will take possesion of the equipment and place in its designated area. **Laptop1: TEB # BB51184691 / Serial # 37240147333** **Laptop2: TEB # BB24646591 / Serial # 7292928457** **OS DVD (release 20170403): TEB # BB46592073**		

Laptop Setup

Step	Activity	Initials	Time
2	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 matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM4: TEB # BB51184642 / Serial # H1411006** **Laptop4: TEB # BB81420138 / Service Tag # F8SVSG2** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46592066**		
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 whether the external display works, then 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**		

Printer Setup

Step	Activity	Initials	Time
5	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`**[2]		

Date Setup

Step	Activity	Initials	Time
6	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 "20190227 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.		

Format and label the blank FD

Step	Activity	Initials	Time
7	CA performs the following steps to format a new FD: a) Plug a new FD into an available USB port in the laptop and wait for it to be recognized. b) Close the file system popup window. CA uses the terminal window to perform the following steps: c) Confirm the drive letter by executing: **`df`** d) Unmount the drive by executing: **`umount /dev/sdb1`** e) Format and label the FD by executing: **`mkfs.vfat -n HSMFD -I /dev/sdb1`** f) CA removes the FD, then places it on the holder.		
8	CA repeats step 7 for the 2nd blank FD.		
9	CA repeats step 7 for the 3rd blank FD.		
10	CA repeats step 7 for the 4th blank FD.		
11	CA repeats step 7 for the 5th blank FD.		

Connect the HSMFD

Step	Activity	Initials	Time
12	CA plugs the **Ceremony 34 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. d) Give the unused **HSMFD 34** to IW.		
13	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: **`hsmfd-hash[3] -c`** IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 34 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.** SHA-256: 227eade2b8661683fc6581e841615a47bd24e29e2c29c656585ef2144feac6a6 PGP Words: blockade insurgent ringbolt tomorrow select gossamer backward Jamaica wayside glossary minnow typewriter cranky frequency enlist determine skullcap Capricorn tiger onlooker Burbank certify southward escapade endorse finicky uproot belowground dropper undaunted southward paragon		

Start the Terminal Session Logging

Step	Activity	Initials	Time
14	CA executes the command below using the terminal window to change the working directory to HSMFD: **`cd /media/HSMFD`**		
15	CA executes the command below to log activities of the **Commands** terminal window: **`script script-20190227.log`**		

Start the HSM Activity Logging

Step	Activity	Initials	Time
16	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`[4] **`/dev/ttyS0`** **Note: DO NOT unplug the serial 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
17	CA performs the following steps to prepare the HSM: a) Plug the serial null modem serial cable to the HSM. b) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** c) Scroll the logging screen up and look for the HSM serial number. d) IW matches the displayed HSM serial number on the screen with the information below. **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).

The CA activates the HSM using the TCR's cards. After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop. The ksrsigner application then uses the private key stored in the HSM to generate the SKR. The SKR contains the digital signatures of the ZSK set to be used in the next quarter. The CA then prints the signer log, backs up the newly created SKR, and deactivates the HSM.

Enable/Activate the HSM (Tier 7)

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 opens the TEB, then gives the plastic case and card to the CA. c) CA keeps the plastic case, then places the card on the card holder that is visible to everyone. **CO1: Arbogast Fabian** **OP TEB # BB46592057** **CO2: Dmitry Burkov** **OP TEB # BB46592058** **CO3: Joao Damas** **OP TEB # BB46592048** **CO4: Carlos Martinez** **OP TEB # BB46592050** **CO5: Olafur Gudmundsson** **OP TEB # BB46592051** **CO6: Nicolas Antoniello** **OP TEB # BB46592060** **CO7: Subramanian Moonesamy** **OP TEB # BB46592063**		
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 #?"** 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 the used cards below. Each card is returned to 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 port.		
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`[5] 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 2019 Q2

Step	Activity	Initials	Time
6	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[6] `/media/KSR/KSK36/ksr-root-2019-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 2019 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. b) IW retains the documents provided by the RZM representative and writes the name: _____ 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 readout, 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 on: **`/media/KSR/KSK36/skr-root-2019-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`**[7] **`ksrsigner-201902*.log`**		
12	IW attaches a copy of each 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) Flush the system buffers by executing: **`sync`** e) 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 #?"** 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 the used cards below. Each card is returned to 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.**		

Test the Unused OP Card

Step	Activity	Initials	Time
16	CA switches to the **HSM Output** terminal window.		
17	CA performs the following steps to test the unused OP card's readability: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"8.View Cards"**, press **ENT** to confirm. c) Insert the OP card from the card holder, then press **ENT** to confirm. d) Verify that **"OP"** is displayed on the HSM, then press **ENT 4 times** to display the information on the terminal window. e) Remove the OP card and return to the card holder. f) Press **CLR** to return to the previous menu. IW records the used cards below. The card is returned to card holder after use. OP card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Act 4. Secure Hardware

The CA backs up the HSMFD contents, prints log information, and places the equipment and TCRs cards inside of TEBs. The CA and IW then escort the SSCs and TCRs into Tier 5 (Safe Room) to return the equipment to Safe #1 and TCRs cards to Safe #2.

Return the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
1	CA switches the HSM to power OFF, then disconnects the power, serial and ethernet connections from it. **Note: DO NOT unplug the cable connections on the laptop.**		
2	CA places the HSM into a prepared TEB, then seals it.		
3	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 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 # BB51184671 / Serial # H1411006**		

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
4	CA performs the following steps to stop logging: a) Disconnect the serial null modem cable 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.**		

Back up the HSMFD Contents

Step	Activity	Initials	Time
5	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: **`shopt -s dotglob`**		
6	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[3] -p`** **Note: One copy for audit bundle and one copy for HSMFD package.**		
7	CA executes the command below using the terminal window to display the contents of the HSMFD: **`ls -ltrR`**		
8	CA plugs a blank FD labeled HSMFD into a free USB slot on the laptop, then waits for the OS to recognize it as **HSMFD1**		
9	CA closes the file system window, then executes the command below to back up the HSMFD: **`cp -pR * /media/HSMFD1`**		
10	CA executes the command below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy: **`hsmfd-hash[3] -m`**		
11	CA executes the command below using the terminal window to unmount the HSMFD copy: **`umount /media/HSMFD1`**		
12	CA removes the **HSMFD1**, then places it on the holder.		
13	CA repeats step 8 to 12 for the 2nd copy.		
14	CA repeats step 8 to 12 for the 3rd copy.		
15	CA repeats step 8 to 12 for the 4th copy.		
16	CA repeats step 8 to 12 for the 5th copy.		

Print Logging Information

Step	Activity	Initials	Time
17	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-201902*.log`** c) **`enscript -Gr --font="Courier8" ttyaudit-tty*-201902*.log`** Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**		

Return HSMFDs and OS DVDs into a TEB

Step	Activity	Initials	Time
18	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.		
19	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, display, and network.		
20	CA places 2 HSMFDs, 2 OS DVDs, 1 sheet of paper paper with the printed HSMFD hash into a prepared TEB, then seals it.		
21	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 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 # BB46584695**		

Distribute the HSMFDs

Step	Activity	Initials	Time
22	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and for process review).		

Return the Laptop into a TEB

Step	Activity	Initials	Time
23	CA places the laptop into a prepared TEB, then seals it.		
24	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 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 # BB81420103 / Service Tag # F8SVSG2**		

Returns HSM Cards into TEBs

Step	Activity	Initials	Time
25	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 OP card to the CO. h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. i) CO writes the date, time, and signature on the table of IW's script, then IW initials the entry. j) CO returns to their seat with the TEB, being especially careful not to compromise it. k) Repeat steps for all the remaining COs on the list. **CO1: Arbogast Fabian** **OP TEB # BB46592089** **CO2: Dmitry Burkov** **OP TEB # BB46592090** **CO3: Joao Damas** **OP TEB # BB46592091** **CO4: Carlos Martinez** **OP TEB # BB46592092** **CO5: Olafur Gudmundsson** **OP TEB # BB46592093** **CO6: Nicolas Antoniello** **OP TEB # BB46592094** **CO7: Subramanian Moonesamy** **OP TEB # BB46592106**		

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	OP 1 of 7	BB46592089	Arbogast Fabian		2019 Feb __		
CO2	OP 2 of 7	BB46592090	Dmitry Burkov		2019 Feb __		
CO3	OP 3 of 7	BB46592091	Joao Damas		2019 Feb __		
CO4	OP 4 of 7	BB46592092	Carlos Martinez		2019 Feb __		
CO5	OP 5 of 7	BB46592093	Olafur Gudmundsson		2019 Feb __		
CO6	OP 6 of 7	BB46592094	Nicolas Antoniello		2019 Feb __		
CO7	OP 7 of 7	BB46592106	Subramanian Moonesamy		2019 Feb __		

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

Step	Activity	Initials	Time
26	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
27	SSC1 opens Safe #1 while shielding the combination from the camera.		
28	SSC1 removes the safe log, then writes the date, time, and signature on 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.**		
29	CA performs the following steps to return each piece of 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 # BB51184671 / Serial # H1411006** **Laptop4: TEB # BB81420103 / Service Tag # F8SVSG2** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584695**		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
30	SSC1 writes the date, time, and signature on the safe log where Close Safe is indicated. IW verifies the entry, then initials it.		
31	SSC1 returns the safe log back to Safe #1 and locks it by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the “WAIT” light indicator is off.		
32	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and closing the door behind them.		

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
33	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)		
34	SSC2 opens Safe #2 while shielding the combination from the camera.		
35	SSC2 removes the safe log, then writes the date, time, and signature on 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
36	The selected CO returns the TEBs by performing the steps below sequentially: a) CO reads aloud the TEB number, then verifies its integrity while showing it 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 TEBs inside it, then locks it. d) CO writes the date, time, and signature on the safe log where "Return OP Card" is indicated. e) IW verifies the completed safe log entry, then initials it. **CO1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46592089** **CO2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46592090** **CO3: Joao Damas** **Box # 1071** **OP TEB # BB46592091** **CO4: Carlos Martinez** **Box # 1068** **OP TEB # BB46592092** **CO5: Olafur Gudmundsson** **Box # 1789** **OP TEB # BB46592093** **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46592094** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46592106**		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
37	Once all relevant deposit boxes are closed and locked, SSC2 writes the date, time, and signature on the safe log where Close Safe is indicated. IW verifies the safe log entry, then initials it.		
38	SSC2 returns the safe log back to Safe #1 and locks it 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 ìWAITî light indicator is off.		
39	CA, IW, SSC2, and COs leave safe room closing the door behind them.		

Act 5. Close the Key Signing Ceremony

The CA will finish the ceremony by:

- Reading any exceptions that may have 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 the exceptions that may have 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 participants have completed.		

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.		

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

Step	Activity	Initials	Time
7	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.)		
8	CA notifies the SA to stop the audit camera video recording.		

Bundle Audit Materials

Step	Activity	Initials	Time
9	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: **20180815 00:00:00 to 20190228 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 36**, 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] **`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*

[3] **`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`[8]
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*

[4] **`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*

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

[6] **`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

[7] **`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*

[8] **`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

---

* 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 may have occurred were accurately and properly documented.

IW: **Yuko Green**

Signature: _____

Date: 2019 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: **20180815 00:00:00 to 20190228 00:00:00 UTC.**

SA: _____

Signature: _____

Date: 2019 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: 2019 Feb __