# Root DNSSEC KSK Ceremony 34

Wednesday August 15, 2018

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 | | | |
| IW | Patrick Jones / ICANN | | | |
| SSC1 | Anand Mishra / ICANN | | | |
| SSC2 | Jessica Castillo / ICANN | | | |
| CO1 | Arbogast Fabian | | | |
| CO2 | Dmitry Burkov | | | |
| CO6 | Nicolas Antoniello | | | |
| CO7 | Subramanian Moonesamy | | | |
| RZM | Ryan Brown / Verisign | | | |
| RZM | Trevor Davis / Verisign | | | |
| RZM | Duane Wessels / Verisign | | | |
| AUD | Catherine Choy / RSM | | 2018 Aug __ | |
| AUD | Micah Springer / RSM | | | |
| SA | Connor Barthold / ICANN | | | |
| SA | Mike Brennan / ICANN | | | |
| RKOS / CA Backup | Alberto Duero / PTI | | | |
| RKOS / IW Backup | Andres Pavez / PTI | | | |
| SW | Leticia Castillo / ICANN | | | |
| SW | Joseph Restuccia / ICANN | | | |
| SW | Laura Bengford / ICANN | | | |
| SW | Matthew Larson / ICANN | | | |
| SW | Paula Wang / PTI | | | |
| SW | David Prangnell / PTI | | | |
| SW | Kim Davies / PTI | | | |
| | | | | |
| | | | | |

***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.***

Note: 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 the Ceremony room if participants are present in the room. CAs, IWs or SAs may escort participants out of the 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 the Ceremony room using the visitor log. The SA starts filming before the participants enter the Ceremony room.

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

| 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

## Sign into the 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 the Ceremony Room, then performs a roll call using the list of participants on page 2. | | |

## Emergency Evacuation Procedures and Electronics Policy

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3 | CA reviews the emergency evacuation procedure with onsite participants. | | |
| 4 | CA explains the use of personal electronic devices during ceremony. | | |
| 5 | CA briefly explains the purpose of the ceremony. | | |

## Verify the Time and Date

| Step | Activity | Initials | Time |
|---|---|---|---|
| 6 | IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room:<br><br>Date and time: _____<br><br>All entries into this script or any logs should follow this common source of time. | | |

## Open the Credential Safe #2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 7 | CA and IW brings a flashlight and escorts the SSC2 and the COs into the safe room. | | |
| 8 | SSC2 opens Safe #2 while shielding the combination from the camera. | | |
| 9 | Perform the following steps to complete the safe log:<br>  a) SSC2 takes out the existing safe log, then shows the most recent page to the audit camera.<br>  b) IW provides the pre-printed safe log to SSC2.<br>  c) SSC2 writes the date, time and signature on the safe log where "Open Safe" is indicated.<br>  d) IW verifies the entry then initials it. | | |

## COs Extract the Credentials From the Safe Deposit Boxes

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 10 | One by one, the selected CO performs the following steps to retrieve the required TEBs:<br><br>a) With the assistance of the CA (and the common key), the CO opens his/her safe deposit box.<br>**Note: Common Key is for the bottom lock. CO Key is for the top lock.**<br>b) CO reads out the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB.<br>c) CO reads out the TEB numbers, then verifies its integrity while showing it to the audit camera above.<br>d) CO retains the TEB specified below, then locks the safe deposit box.<br>e) CO writes the date, time and signature on the safe log where removal of TEBs are indicated.<br>f) IW verifies the completed safe log entries, then initials it.<br><br>**CO1: Arbogast Fabian**<br>**Box # 1791**<br>**OP TEB # BB46592046 (Retain)**<br>**SO TEB # BB46584451 (Check and Return)**<br><br>**CO2: Dmitry Burkov**<br>**Box # 1793**<br>**OP TEB # BB46592047 (Retain)**<br>**SO TEB # BB46584453 (Check and Return)**<br><br>**CO6: Nicolas Antoniello**<br>**Box # 1073**<br>**OP TEB # BB46592052 (Retain)**<br>**SO TEB # BB46584459 (Check and Return)**<br><br>**CO7: Subramanian Moonesamy**<br>**Box # 1792**<br>**OP TEB # BB46592053 (Retain)**<br>**SO TEB # BB46584461 (Check and Return)** | | |

## Close the Credential Safe #2

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 11 | 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. | | |
| 12 | SSC2 returns the safe log back in the Safe #2 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW verifies that the safe is locked and the "WAIT" light indicator is off. | | |
| 13 | CA, IW, SSC2, and COs leave the safe room with TEBs, closing the door behind them. | | |

## Open Equipment Safe #1

| Step | Activity | Initials | Time |
|---|---|---|---|
| 14 | CA and IW brings a cart and escorts the SSC1 into the safe room. | | |
| 15 | SSC1 opens Safe #1 while shielding the combination from the camera. | | |
| 16 | Perform the following steps to complete the safe log:<br><br>a) SSC1 takes out the existing safe log, then shows the most recent page to the audit camera.<br><br>b) IW provides the pre-printed safe log to SSC1.<br><br>c) SSC1 writes the date, time and signature on the safe log where "Open Safe" is indicated.<br><br>d) IW verifies the entry then initials it. | | |

## Remove the Equipment from Safe #1

| Step | Activity | Initials | Time |
|---|---|---|---|
| 17 | CA performs the following steps to extract each equipment from the safe:<br><br>a) CAREFULLY remove each equipment TEB from the safe.<br><br>b) Read out each TEB number, then verify its integrity while showing it to the audit camera.<br><br>c) Place each equipment TEB on the cart as specified on the list below.<br><br>d) Write the date, time and signature on the safe log where "Remove" is indicated.<br><br>e) IW verifies the safe log entry, then initials it.<br><br>**HSM3: TEB # BB51184623 / Serial # H1403033 (Place on cart)**<br>**HSM4: TEB # BB51184642 / Serial # H1411006 (Check and Return)**<br><br>**Laptop1: TEB # BB51184640 / Serial # 37240147333 (Place on cart)**<br>**Laptop2: TEB # BB24646591 / Serial # 7292928457 (Check and Return)**<br>**Laptop3: TEB # BB81420139 / Service Tag # C8SVSG2 (Place on cart)**<br>**Laptop4: TEB # BB81420138 / Service Tag # F8SVSG2 (Check and Return)**<br><br>**OS DVD (release 20170403) + HSMFD: TEB # BB46592049 (Place on cart)**<br><br>**Note: The Service Tag # is the same as the Serial Number.** | | |

## Close the Equipment Safe #1 and exit the Safe Room

| Step | Activity | Initials | Time |
|---|---|---|---|
| 18 | SSC1 writes the date, time and signature on the safe log where Close Safe is indicated.<br>IW verifies the safe log entry then initials it. | | |
| 19 | SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise).<br>CA and IW verifies that the safe is locked and the "WAIT" light indicator is off. | | |
| 20 | CA, IW and SSC1 leaves the safe room with the cart, closing the door behind them. | | |

# Act 2. OS DVD Acceptance Test

## Setup Equipment

| Step | Activity | Initials | Time |
|:---:|---|---|---|
| **1** | CA performs the following steps to prepare the listed equipment:<br>    a) Remove the equipment TEBs from the cart and place them on the ceremony table.<br>    b) Inspect each equipment TEB for tamper evidence.<br>    c) Read out the TEB number and the serial number (if applicable) while IW matches it with the prior ceremony script in this facility.<br>    d) Remove and discard the TEB, then place the equipment on its designated area on the ceremony table.<br><br>**Laptop1: TEB # BB51184640 / Serial # 37240147333**<br>**OS DVD (release 20170403) + HSMFD: TEB # BB46592049** | | |
| **2** | CA performs the following steps to boot the laptop:<br>    a) Connect the USB of the general purpose external DVD drive.<br>    b) Connect the external display, then the power supply.<br>    c) Immediately insert the **OS DVD release 20170403** into the laptop DVD try after the laptop power is switched ON. | | |
| **3** | CA performs the following steps to setup the laptop:<br>    a) Press `Ctrl+Alt+F2` to get a console prompt and log in as `root`<br>    b) Execute `system-config-display --noui`<br>    c) Execute `killall Xorg`<br>    d) Confirm that the external display works.<br>    e) Log in as `root` | | |
| **4** | CA opens a terminal window through:<br>**Applications > Accessories > Terminal**<br>CA performs the following steps to increase its visibility:<br>    a) Click the **View** menu and select **Zoom In.**<br>    b) Repeat the step above as necessary. | | |

# OS DVD Acceptance Test

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 5 | CA inserts the new **OS DVD release coen-0.4.0** into the external DVD drive, waits for it to be recognized by the OS, then performs the following steps:<br><br>   a) Close the file system popup window.<br><br>CA uses the terminal window to continues with the following steps:<br><br>   b) Confirm the drive letter by executing:<br>     `df`<br>   c) Unmount the drive by executing:<br>     `umount /dev/scd1`<br>   d) Calculate the SHA-256 hash by executing:<br>     `sha2wordlist < /dev/scd1`<br><br>IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.<br>**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.**<br><br>SHA-256 hash:<br>**8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f**<br><br>PGP Words:<br>**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**<br><br>**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/34** | | |
| 6 | CA removes the OS DVD by pressing the eject button on the external DVD drive, then places it on the ceremony table.<br>**Note: The tested OS DVD must be placed on the ceremony table where it is visible to the audit camera and the participants** | | |
| 7 | CA repeats step 5 to 6 for the 2<sup>nd</sup> copy of the new **OS DVD release coen-0.4.0.** | | |
| 8 | IW records his/her signature upon successful completion of the<br>**OS DVD release coen-0.4.0** acceptance testing.<br><br><br>Printed Name: **Patrick Jones**<br><br>Signature: _____<br><br><br>Date: **2018/08/15** | | |

# Return the OS DVDs and Laptop to TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 9 | CA performs the following steps to switch OFF the laptop and remove the OS DVD:<br><br>a) Turn OFF the laptop by pressing the power switch button.<br><br>b) Turn ON the laptop and immediately remove the OS DVD from it.<br><br>c) Disconnect all connections from the laptop including power, display and external DVD drive. | | |
| 10 | CA performs the following steps to return the equipment to TEB:<br><br>a) CA places 2 **OS DVD release 20170403** into a prepared TEB, then seals it.<br><br>b) CA places the Laptop1 into a prepared TEB, then seals it. | | |
| 11 | CA performs the following steps to verify the TEBs:<br><br>a) Read out the TEB number, then show it to the audit camera above for participants to see.<br><br>b) Confirm with IW that the TEB number matches with the information below.<br><br>c) Initial the TEB with IW using a ballpoint pen.<br><br>d) Give IW the sealing strips for later inventory.<br><br>e) Place the TEB on the cart.<br><br>**OS DVD release 20170403: TEB # BB46592068**<br>**Laptop1: TEB # BB51184666 / Serial # 37240147333** | | |

# Act 3. Setup Equipment

## Setup Laptop

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | CA performs the following steps to prepare the listed equipment:<br>a) Remove all equipment TEBs from the cart and place them on the ceremony table.<br>b) Inspect each equipment TEB for tamper evidence.<br>c) Read out the TEB number and the serial number (if applicable) while IW matches it with the prior ceremony script in this facility.<br>d) Remove and discard the TEB, then place the equipment on its designated area on the ceremony table.<br><br>**HSM3: TEB # BB51184623 / Serial # H1403033**<br>**Laptop3: TEB # BB81420139 / Serial # C8SVSG2** | | |
| 2 | CA performs the following steps to boot the laptop:<br>a) Connect the USB printer cable into the back USB slot of the laptop.<br>b) Connect the Null Modem cable into the Serial Port of the laptop.<br>c) Connect the external HDMI display.<br>d) Connect the power supply.<br>e) Immediately insert the **OS DVD release coen-0.4.0** after the laptop power is switched ON. | | |
| 3 | CA verifies if the external display works, then perform adjustments if necessary:<br>To change the font size of the terminal:<br>Click the **View** menu and select **Zoom In** or **Zoom Out**<br>To change the resolution of each screen:<br>Go to **Applications > Settings > Display** | | |

## Setup Printer

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4 | 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:<br>`configure-printer` | | |

## Setup Date

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5 | CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock.<br><br>If the date/time do not match, perform the following steps:<br>a) Execute `date -s "20180815 HH:MM:00"` to set the time.<br>where HH is two-digit hour, MM is two-digit minutes and 00 is zero seconds.<br>b) Execute `date` to confirm the date/time matches the clock. | | |

# Format and label the blank FD

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 6 | CA performs the following steps to format a new FD:<br><br>    a) Plug a new FD into the USB slot of the laptop and wait for it to be recognized.<br>    b) Close the file system popup window.<br><br>CA uses the terminal window to continue with the following steps:<br><br>    c) Confirm the drive letter by executing:<br>       `df`<br>    d) Unmount the drive by executing:<br>       `umount /dev/sda1`<br>    e) Format and label the FD by executing:<br>       `mkfs.vfat -n HSMFD -I /dev/sda1`<br>    f) CA removes the FD, then places it on the holder. | | |
| 7 | CA repeats step 6 for the 2nd blank FD. | | |
| 8 | CA repeats step 6 for the 3rd blank FD. | | |
| 9 | CA repeats step 6 for the 4th blank FD. | | |
| 10 | CA repeats step 6 for the 5th blank FD. | | |

# Connect the HSMFD

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 11 | CA plugs the **Ceremony 32 HSMFD** into the USB slot, then performs the following steps:<br><br>    a) Wait for the OS to recognize it.<br>    b) Display the HSMFD contents to all participants.<br>    c) Close the file system window.<br>    d) Give the unused **HSMFD 32** to IW. | | |
| 12 | CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD:<br><br>`hsmfd-hash -c`<br><br>IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 32 annotated script.<br>**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.**<br><br>```
SHA-256:    e3d877c855ec3d1a1f97f07c397e7b75c208f0afa7ef65811b45396d5bb246fe
PGP Words:  tissue stupendous involve retrieval edict unicorn commence Bradbury billiard mosquito unearth informant classroom insurgent kickoff impartial snapshot antenna unearth pharmacy repay unravel fracture inventive beeswax detector classroom hazardous erase pioneer cubic yesteryear
``` | | |

## Start the Terminal Session Logging

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 13 | CA executes the command below using the terminal window to change the default directory to HSMFD:<br>`cd /media/HSMFD` | | |
| 14 | CA executes the command below to log activities of the **Commands** terminal window :<br>`script script-20180815.log` | | |

## Start the HSM Activity Logging

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 15 | CA performs the following steps using the **HSM Output** terminal window to capture the activity logs of the HSM:<br>　a) Change the default directory to HSMFD by executing:<br>　　`cd /media/HSMFD`<br>　b) Set the serial port baud rate by executing:<br>　　`stty -F /dev/ttyS0 115200`<br>　c) Start logging the serial output by executing:<br>　　`ttyaudit /dev/ttyS0`<br>**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

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 16 | CA performs the following steps to prepare the HSM:<br>　a) Plug the serial null modem serial cable to the HSM.<br>　b) Connect the power to the HSM, then switch it ON.<br>　**Note: Status information should appear on the HSM activity logging screen.**<br>　c) Scroll the logging screen up and look for the HSM serial number.<br>　d) IW matches the displayed HSM serial number on the screen with the information below.<br><br>**HSM3: Serial # H1403033**<br>**Note: The date and time on the HSM is not used as a reference for logging and timestamp.** | | |

# Act 4. Activate HSM and Generate Signatures

## Enable/Activate the HSM

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | One by one, CA calls each COs listed below to perform the following steps:<br><br>   a) CO reads out the TEB number, then CA inspects it for tamper evidence.<br>   b) CO opens the TEB, then gives the plastic case and card to the CA.<br>   c) CA keeps the plastic case, then places the card on the card holder that is visible to everyone.<br><br>**CO1: Arbogast Fabian**<br>**OP TEB # BB46592046**<br><br>**CO2: Dmitry Burkov**<br>**OP TEB # BB46592047**<br><br>**CO6: Nicolas Antoniello**<br>**OP TEB # BB46592052**<br><br>**CO7: Subramanian Moonesamy**<br>**OP TEB # BB46592053** | | |
| 2 | CA performs the following steps to activate the **HSM**:<br>   a) Utilize the HSM's keyboard to scroll through the menu using < ><br>   b) Select **"1.Set Online"**, hit **ENT** to confirm.<br>   c) When **"Set Online?"** is displayed, hit **ENT** to confirm.<br>   d) When **"Insert Card OP #?"** is displayed, insert the OP card.<br>   e) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT**.<br>   f) When **"Remove Card?"** is displayed, remove the OP card.<br>   g) Repeat steps d) to f) for the 2$^{nd}$ and 3$^{rd}$ OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **ON.**<br>IW records the used cards below. Each card is returned to card holder after use.<br>1$^{st}$  OP card _____ of 7<br>2$^{nd}$ OP card _____ of 7<br>3$^{rd}$  OP card _____ of 7<br>**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 Ethernet cable in LAN port. | | |
| 4 | CA performs the following steps to test the network connectivity between laptop and HSM:<br>  a) Use the **Commands** terminal window<br>  b) Test connectivity by executing:<br>  `ping hsm`<br>  c) Wait for responses, then exit by pressing:<br>  `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.<br>**Note: The KSR FD was transferred to the facility by the RKOS. It contains 4 KSRs. 1 for normal operation and the rest for fallback scenario(s).** | | |

## Execute the KSR Signer for Phase D to E

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 6 | CA executes the command below on the terminal window to sign the KSR file:<br>`ksrsigner /media/KSR/KSK34-0-D_to_E/ksr-root-2018-q4-0-d_to_e.xml` | | |
| 7 | When the KSR signer displays the prompt:<br>`Activate HSM prior to accepting in the affirmative!! (y/N):`<br>CA confirms that the HSM is online, then enters **"y"** to proceed. | | |

## Verify the KSR Hash for Phase D to E

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 8 | When the hash of the KSR is displayed on the terminal window, perform the following: <br>    a) CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room and provide documents for IW to review. <br>    b) RZM representative reads out the PGP word list SHA-256 hash of the KSR file being used. <br>    c) IW retains the documents provided by the RZM representative and writes the name : <br><br> _____ | | |
| 9 | Participants confirm that the hash displayed on the terminal window matches with the RZM read out, 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/KSK34-0-D_to_E/skr-root-2018-q4-0-d_to_e.xml** | | |

## Execute the KSR Signer for Phase E to D

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 11 | CA executes the command below on the terminal window to sign the KSR file: <br> **ksrsigner /media/KSR/KSK34-1-E_to_D/ksr-root-2018-q4-1-e_to_d.xml** | | |
| 12 | When the KSR signer displays the prompt: <br> **Activate HSM prior to accepting in the affirmative!! (y/N):** <br> CA confirms that the HSM is online, then enters **"y"** to proceed. | | |

## Verify the KSR Hash for Phase E to D

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 13 | When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. | | |
| 14 | Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"** | | |
| 15 | CA enters **"y"** in response to **"Is this correct (y/N)?"** to complete the KSR signing operation. The SKR is located on: **/media/KSR/KSK34-1-E_to_D/skr-root-2018-q4-1-e_to_d.xml** | | |

## Execute the KSR Signer for Phase D to D

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 16 | CA executes the command below on the terminal window to sign the KSR file:<br>`ksrsigner /media/KSR/KSK34-2-D_to_D/ksr-root-2018-q4-2-d_to_d.xml` | | |
| 17 | When the KSR signer displays the prompt:<br>`Activate HSM prior to accepting in the affirmative!! (y/N):`<br>CA confirms that the HSM is online, then enters **"y"** to proceed. | | |

## Verify the KSR Hash for Phase D to D

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 18 | When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. | | |
| 19 | Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"** | | |
| 20 | CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located on:<br>`/media/KSR/KSK34-2-D_to_D/skr-root-2018-q4-2-d_to_d.xml` | | |

## Execute the KSR Signer for Phase C to C

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 21 | CA executes the command below on the terminal window to sign the KSR file:<br>`ksrsigner /media/KSR/KSK34-3-C_to_C/ksr-root-2018-q4-3-c_to_c.xml` | | |
| 22 | When the KSR signer displays the prompt:<br>`Activate HSM prior to accepting in the affirmative!! (y/N):`<br>CA confirms that the HSM is online, then enters **"y"** to proceed. | | |

## Verify the KSR Hash for Phase C to C

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 23 | When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. | | |
| 24 | Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"** | | |
| 25 | CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located on:<br>`/media/KSR/KSK34-3-C_to_C/skr-root-2018-q4-3-c_to_c.xml` | | |

# Print Copies of the KSR Signer log

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 26 | CA executes the command below on the terminal window to print the KSR Signer log:<br>`for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i X; done`<br>**Note: Replace "X" with the amount of copies needed for the participants.** | | |
| 27 | IW attaches a copy of each ksrsigner log to his/her script. | | |

# Backup the Newly Created SKR

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 28 | CA executes the following commands on the terminal window to copy the contents of the KSR FD:<br>`cp –pR /media/KSR/* .`<br>Confirm overwrite by entering "y" if prompted. | | |
| 29 | CA executes the following commands on the terminal window:<br>a) list the contents of the KSR FD by executing:<br>`ls –ltrR /media/KSR`<br>b) flush the system buffers by executing:<br>`sync`<br>c) unmount the KSR FD by executing:<br>`umount /media/KSR` | | |
| 30 | CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative. | | |

# Disable/Deactivate the HSM

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 31 | CA ensures to utilize the unused OP cards to deactivate the **HSM**:<br>a) CA displays the HSM activity logging terminal window<br>b) Utilize the HSM's keyboard to scroll through the menu using < ><br>c) Select **"2.Set Offline"**, hit **ENT** to confirm.<br>d) When **"Set Offline?"** is displayed, hit **ENT** to confirm.<br>e) When **"Insert Card OP #?"** is displayed, insert the OP card from the card holder.<br>f) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT**.<br>g) When **"Remove Card?"** is displayed, remove the OP card.<br>h) Repeat steps e) to g) for the 2$^{nd}$ and 3$^{rd}$ OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **OFF.**<br>IW records the used cards below. Each card is returned to card holder after use.<br>1$^{st}$ OP card _____ of 7<br>2$^{nd}$ OP card _____ of 7<br>3$^{rd}$ OP card _____ of 7<br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | | |

# Act 5. Secure Hardware

## Return the HSM to TEB

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 1 | CA switches the HSM to power OFF, then disconnects the power, serial and Ethernet connections from it.<br>**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:<br><br>a) Read out the TEB number and HSM serial number, then shows it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number and HSM serial number match below.<br>c) Initial the TEB with IW using a ballpoint pen.<br>d) Give IW the sealing strips for later inventory.<br>e) Place the HSM TEB on the cart.<br><br>**HSM3: TEB # BB51184667 / Serial # H1403033** | | |

## Stop logging the Serial Output and the Terminal Session

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 4 | CA performs the following steps to stop logging:<br><br>a) Disconnect the serial null modem cable from the laptop.<br>b) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**:<br>Press **Ctrl + C**<br>Execute **exit**<br>c) Execute the command below using the **Commands** terminal window to stop logging the terminal session:<br>**exit**<br>**Note: The Commands terminal session window will remain open.** | | |

# Backup the HSMFD Contents

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 5 | CA executes the command below using the terminal window to set `dotglob`:<br>`shopt -s dotglob`<br>**Note: This enables copying of all files from the original HSMFD.** | | |
| 6 | CA executes the command below **twice** using the terminal window to print **2** copies of the hash:<br>`hsmfd-hash -p`<br>**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:<br>`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 backup the HSMFD:<br>`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:<br>`hsmfd-hash -m` | | |
| 11 | CA executes the command below using the terminal window to unmount the HSMFD copy:<br>`umount /media/HSMFD1` | | |
| 12 | CA removes the **HSMFD1**, then places it on the holder. | | |
| 13 | CA repeats step 8 to 12 for the 2<sup>nd</sup> copy. | | |
| 14 | CA repeats step 8 to 12 for the 3<sup>rd</sup> copy. | | |
| 15 | CA repeats step 8 to 12 for the 4<sup>th</sup> copy. | | |
| 16 | CA repeats step 8 to 12 for the 5<sup>th</sup> copy. | | |

# Print Logging Information

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 17 | CA executes the following commands on the terminal window to print a copy of the logging information:<br>`enscript -2Gr -# 1 script-201808*.log`<br>`enscript -Gr -# 1 --font="Courier8" ttyaudit-tty*-201808*.log`<br>Attach the printed copies to IW script.<br>**Note: Ignore the error regarding non-printable characters if prompted.** | | |

## Place HSMFDs and OS DVDs into the TEB

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 18 | CA executes the following commands on the terminal window to unmount the HSMFD:<br>`cd /tmp`<br>`umount /media/HSMFD`<br>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:<br>a) Remove the OS DVD from the laptop.<br>b) Turn OFF the laptop by pressing the power switch button.<br>c) Disconnect all connections from the laptop including power, printer, display and network. | | |
| 20 | CA places 2 HSMFD, 2 OS DVD, 1 paper with printed HSMFD hash into a prepared TEB, then seals it. | | |
| 21 | CA performs the following steps to verify the TEB:<br>a) Read out the TEB number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number matches with the information below.<br>c) Initial the TEB with IW using a ballpoint pen.<br>d) Give IW the sealing strips for later inventory.<br>e) Place the OS DVD TEB on the cart.<br><br>**OS DVD release coen-0.4.0 + HSMFD: TEB # BB46592066** | | |

## Distribute the HSMFDs

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

## Return the Laptop to TEB

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 23 | CA places the laptop into a prepared TEB, then seals it. | | |
| 24 | CA performs the following steps:<br>a) Read out the TEB number and Laptop serial number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number and Laptop serial number matches with the information below.<br>c) Initial the TEB with IW using a ballpoint pen.<br>d) Give IW the sealing strips for later inventory.<br>e) Place the Laptop TEB on the cart.<br><br>**Laptop3: TEB # BB81420136 / Service Tag # C8SVSG2** | | |

# Return Cards to TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| **25** | One by one, CA calls each COs listed below to the ceremony table to perform the following steps:<br><br>a) CA takes the OP TEB and plastic case prepared for the CO.<br><br>b) CO takes his/her OP card from the card holder and places it inside the plastic case.<br><br>c) CO gives the plastic case containing the OP card to the CA.<br><br>d) CA places the plastic case into the prepared TEB, reads out the TEB number and description, then seals it.<br><br>e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for later inventory.<br><br>f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.<br><br>g) CA gives the TEB containing the OP card to the CO.<br><br>h) CO inspects the TEB, verifies its content, then initials it with a ballpoint pen.<br><br>i) CO writes the date, time and signature on the table of IW's script, then IW initials the entry.<br><br>j) CO returns to his/her seat with the TEB and careful not to poke or puncture the TEB.<br><br>k) Repeat steps for all the remaining COs on the list.<br><br>**CO1: Arbogast Fabian**<br>**OP TEB # BB46592057**<br><br>**CO2: Dmitry Burkov**<br>**OP TEB # BB46592058**<br><br>**CO6: Nicolas Antoniello**<br>**OP TEB # BB46592060**<br><br>**CO7: Subramanian Moonesamy**<br>**OP TEB # BB46592063** | | |

| TCR | Card Type | TEB # | Printed Name | Signature | Date | Time | IW Initials |
|-----|-----------|-------|--------------|-----------|------|------|-------------|
| CO1 | OP 1 of 7 | BB46592057 | Arbogast Fabian | | 2018 Aug __ | | |
| CO2 | OP 2 of 7 | BB46592058 | Dmitry Burkov | | 2018 Aug __ | | |
| CO6 | OP 6 of 7 | BB46592060 | Nicolas Antoniello | | 2018 Aug __ | | |
| CO7 | OP 7 of 7 | BB46592063 | Subramanian Moonesamy | | 2018 Aug __ | | |

# Return the Equipment to Safe #1

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 26 | CA and IW brings a cart and escorts SSC1 into the 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.<br>IW verifies this entry, then initials it.<br>**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 equipment to the Safe:<br>    a) CAREFULLY remove the equipment TEB from the cart.<br>    b) Read out the TEB number while showing it to the audit camera above, then place it inside Safe #1<br>    c) Write the date, time and signature on the safe log where **"Return"** is indicated.<br>    d) IW verifies the safe log entry, then initials it.<br><br>**HSM3: TEB # BB51184667 / Serial # H1403033**<br>**Laptop1: TEB # BB51184666 / Serial # 37240147333 (Place on cart)**<br>**Laptop3: TEB # BB81420136 / Service Tag # C8SVSG2 (Place on cart)**<br>**OS DVD (release 20170403): TEB # BB46592068**<br>**OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46592066** | | |

# Close the Equipment Safe #1

| 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 in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW verifies that the safe is locked and the "WAIT" light indicator is off. | | |
| 32 | CA, SSC1 and IW leaves the safe room with the cart, closing the door behind them. | | |

# Open the Credential Safe #2

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 33 | CA and IW brings a flashlight and escorts the SSC2 and the COs into the 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.<br>IW verifies this entry, then initials it.<br>**Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** | | |

## CO Returns the Credentials to Safe #2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 36 | One by one, the selected CO returns the TEBs by performing the following steps below:<br><br>a) CO reads out the TEB number, then verifies its integrity while showing it to the audit camera above<br><br>b) With the assistance of the CA (and the common key), the CO opens his/her safe deposit box.<br>**Note: Common Key is for the bottom lock. CO Key is for the top lock.**<br><br>c) CO reads out the safe deposit box number, places his/her TEBs inside it, then locks it.<br><br>d) CO writes the date, time and signature on the safe log where "Return OP Card" is indicated.<br><br>e) IW verifies the completed safe log entry, then initials it.<br><br>**CO1: Arbogast Fabian**<br>**Box # 1791**<br>**OP TEB # BB46592057**<br><br>**CO2: Dmitry Burkov**<br>**Box # 1793**<br>**OP TEB # BB46592058**<br><br>**CO6: Nicolas Antoniello**<br>**Box # 1073**<br>**OP TEB # BB46592060**<br><br>**CO7: Subramanian Moonesamy**<br>**Box # 1792**<br>**OP TEB # BB46592063** | | |

## Close the Credential Safe #2

| 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 #2, then locks it (spin dial must go at least two full revolutions each way, counter clock-wise then clock-wise). CA and IW verifies that the safe is locked and the "WAIT" light indicator is off. | | |
| 39 | CA, IW, SSC2, and COs leave safe room closing the door behind them. | | |

# Act 6. Close the Key Signing Ceremony

## 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.** IW signs the list and records the completion time once all participants have completed. | | |
| 3 | CA reviews IW's script, then signs the participants list. | | |

## Stop Online Streaming

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 4 | CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming. | | |

## Post Ceremony Information

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 5 | CA informs onsite participants about post ceremony activities. | | |

## Sign Out of Ceremony Room and Stop Video Recording

| Step | Activity | Initials | Time |
|------|----------|----------|------|
| 6 | RKOS ensures that all participants are signed out of the Ceremony Room log and escorted out of the Ceremony Room. SA, IW and CA must remain in the Ceremony Room. | | |
| 7 | CA notifies the SA to stop the audit camera video recording. | | |

# Bundle Audit Materials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 8 | IW makes a copy of his/her script for off-site audit bundle. Each Audit bundle contains:<br><br>a) Output of signer system – HSMFD.<br><br>b) Copy of IW's key ceremony script.<br><br>c) Audio-visual recording from the audit cameras.<br><br>d) Logs from the Physical Access Control System and Intrusion Detection System:<br>Range: **20180207 00:00:00 to 20180816 00:00:00 UTC**<br><br>e) IW's attestation (Appendix B).<br><br>f) SA's attestation (Appendix C and D).<br><br>All TEBs are labeled **Root DNSSEC KSK Ceremony 34**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage. | | |

# Appendix A. Audit Bundle Checklist

## A.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

## A.2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes during the ceremony and attestation. See Appendix B.

## A.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.

## A.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.

## A.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 C.

## A.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 D. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

## A.7. Other items

If applicable.

# Appendix B. 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: **Patrick Jones**

Signature:

_____

Date: 2018 Aug __

# Appendix C. 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: **20180207 00:00:00 to 20180816 00:00:00 UTC.**

SA:

_____

Signature:

_____

Date: 2018 Aug \_\_

# Appendix D. 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: 2018 Aug \_\_