Root DNSSEC KSK Ceremony 38

Wednesday August 14, 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	Francisco Arias / ICANN			
IW	Jonathan Denison / ICANN			
SSC1	Anand Mishra / ICANN			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO5	Olafur Gudmundsson			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Trevor Davis / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Miguel Angel Silvestre / RSM		2019 Aug —	
AUD	Jun Jian Lin / RSM			
SA	Brian Martin / ICANN			
SA	Patrick Tudor / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Peter Elsesser / ICANN			
EW	Ben Filiaipulotu Pepa			
EW	Sergey Rimsha			
EW	Chait Nelakanti			
EW	Julian Livingston Macassey			
EW	Tom Arnfeld			

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 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 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 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 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 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 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.		
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	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 their integrity while showing them to the audit camera above. d) CO retains the TEB(s) specified below, then locks the safe deposit box. e) CO writes the date and time, then signs the safe log where removal of a TEB is indicated. f) IW verifies the completed safe log entries, then initials it. **CO1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46592089 (Retain)** **SO TEB # BB46584451 (Retain)** **CO2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46592090 (Retain)** **SO TEB # BB46584453 (Retain)** **CO5: Olafur Gudmundsson** **Box # 1789** **OP TEB # BB46592093 (Retain)** **SO TEB # BB46584666 (Retain)** **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46592094 (Retain)** **SO TEB # BB46584459 (Retain)** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46592106 (Retain)** **SO TEB # BB46584461 (Retain)**		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
12	Once all safety 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 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 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. **HSM1: TEB # BB51184701 (Place on Cart)** **HSM2: TEB # BB24646624 (Place on Cart)** **HSM3: TEB # BB51184667 (Place on Cart)** **HSM4: TEB # BB51184671 (Place on Cart)** **HSM5W: TEB # BB51184509 (Place on Cart)** **Laptop3: TEB # BB81420136 (Place on Cart)** **Laptop4: TEB # BB81420103 (Check and Return)** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584695 (Place on Cart)** **KSK-2010: TEB # BB46584332 (Place on Cart)** **KSK-2017: TEB # BB46584449 (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 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. Dismantle the Zeroized Hardware Security Module

As part of the HSM lifecycle, previously zeroized HSMs will have their critical components removed and securely destroyed.

- CA will intentionally tamper the HSM
- CA will dismantle the HSM and extract the critical components
- CA will place the components into a TEB in preparation for offsite secure destruction

Prepare HSM for Dismantling

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the HSM equipment listed below: a) Remove HSM TEB from the cart and place it on the ceremony table. b) Inspect HSM TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW matches them with the prior ceremony script in this facility. d) Remove and discard the TEB. **HSM2: TEB # BB24646624 / Serial # K6002018** **Last Verified: KSK32 2018-02-07**		
2	CA performs the following steps to tamper the HSM equipment listed below: a) Connect the power to the HSM, then wait for it to display **"Important Read Manual"** indicating the HSM is in the initialized state. b) Using **Tool B**, press and hold the recessed button on the rear panel of the HSM located between the LAN and serial ports, then release it after 10 seconds to activate the tampering mechanism. c) Press the **RESTART** button on HSM and wait until the **ALERT** LED light is **ON**. d) Disconnect the power from the HSM. **HSM2: Serial # K6002018** Note: The HSM is tampered when the ALERT LED is ON.		

Open Case and Remove Logic Board from HSM2

Step	Activity	Initials	Time
3	IW reads steps 4 to 7 while the CA dismantles **HSM2: Serial # K6002018**.		
4	CA performs the following steps to access and extract the HSM's critical components: a) Using **Tool A+Bit 2**, remove the 2 screws that secure the serial port to the rear panel. b) Using **Tool A+Bit 3**, remove the 2 screws that secure the power port to the rear panel. c) Using **Tool A+Bit 1**, remove the 4 screws from the rear panel of the case that secure the shell. d) Using **Tool A+Bit 1**, remove the 4 screws from the bottom of the case that secure the shell. e) Using **Tool C**, slice the tamper stickers on the bottom of the case. f) Slide the shell toward the back of the case to remove it and place it in the **HSM Parts** bin on the ceremony table. g) Using **Tool A+Bit 3**, remove the 2 logic board screws nearest to the front panel that secure the plastic cover. h) Remove the plastic logic board cover and place it in the **HSM Parts** bin on the ceremony table. i) Using **Tool A+Bit 3**, remove the remaining 2 screws that hold the logic board near the rear panel. j) Detach the 4 cables from the front of the logic board, unlocking the latches by opening them outward to release the 2 ribbon cables.		
5	CA performs the following steps to remove the logic board and battery: a) Using **Tool D**, cut the 2 zip ties near the rear panel. b) Separate the logic board from the HSM case by pulling the logic board up and forward on the right side first to get the battery past the cryptographic module, then flipping it open to the left. c) Using **Tool C**, cut the copper ribbon cable between the cryptographic module and the logic board. d) Using **Tool D**, cut the green cable between the cryptographic module and the logic board. e) Using **Tool D**, cut the battery terminals that connect the battery to the logic board, and remove the zip ties. f) Pry the battery from the logic board by setting the logic board flat on the table and pulling up on the battery with sufficient force to break the adhesive bond. g) Place the battery in the **HSM Parts** bin on the ceremony table. h) Place the logic board in the **Critical Parts** area of the ceremony table.		

Remove Cryptographic Module and Card Reader from HSM2

Step	Activity	Initials	Time
6	CA performs the following steps to remove the cryptographic module: a) Using **Tool E**, remove the 4 nuts that secure the cryptographic module to the case. b) Lift the cryptographic module up to separate it from the case. c) Place the cryptographic module in the **Critical Parts** area of the ceremony table.		
7	CA performs the following steps to remove the front panel and card reader: a) Using **Tool A+Bit 4**, remove the 4 nuts that 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 that secures the card reader. d) Using **Tool A+Bit 3**, remove the 3 screws that secure the card reader. e) Press the ribbon cable down against the case near the connector while pulling up with sufficient force on the card reader to remove it from the case. f) Place the ribbon cable and HSM case in the **HSM Parts** bin on the ceremony table. g) Place the card reader in the **Critical Parts** area of the ceremony table.		

Place the Critical HSM2 parts into a TEB

Step	Activity	Initials	Time
8	CA collects the following parts from the HSM and places them into a prepared TEB, then seals it. a) Cryptographic Module b) Logic Board c) Card Reader **Note: The logic board should be wrapped in foam to prevent accidentally puncturing the TEB. The HSM case will not be destroyed.**		
9	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. **HSM2: TEB # BB51184510**		

Prepare Previously Dismantled HSM for Offsite Destruction

Step	Activity	Initials	Time
10	CA performs the following steps for the HSM equipment listed below: a) Remove HSM TEB from the cart and place it on the ceremony table. b) Inspect HSM TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW matches them with the prior ceremony script in this facility. d) Give RKOS the TEB for destruction. **HSM1: TEB # BB51184701** **Last Verified: KSK32 2018-02-07**		

Act 3. 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
- 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)

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 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. **HSM3: TEB # BB51184667 / Serial # H1403033** **Last Verified: KSK36 2019-02-27** **Laptop3: TEB # BB81420136 / Service Tag # C8SVSG2** **Last Verified: KSK36 2019-02-27** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584695** **Last Verified: KSK36 2019-02-27**		
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 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**		

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/38		

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 "20190814 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

8	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.		

9	CA repeats step 8 for the 2nd blank FD.		
10	CA repeats step 8 for the 3rd blank FD.		
11	CA repeats step 8 for the 4th blank FD.		
12	CA repeats step 8 for the 5th blank FD.		

Connect the HSMFD

Step	Activity	Initials	Time

13	CA plugs the **Ceremony 36 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.		

14	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 36 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 2019/02/27
	
	 # find -P /media/HSMFD/ -type f -print0
		sort -z	xargs -0 cat	sha2wordlist
				
				 SHA-256: 4e232aa80a5156480ed53f761221636c9f5a101ef10d9073e16c754bd2177ef8
				PGP Words: drifter cannonball brickyard paramount allow enchanting egghead dictator apple
				specialist cowbell impetus atlas Camelot flatfoot handiwork quota existence assume Burlingt
				on unwind asteroid peachy hurricane tempest handiwork indulge disable standard bookseller l
				ocale warranty
				``		

Distribute Previous HSMFD

Step	Activity	Initials	Time
15	CA gives the unused **HSMFD 36** and the sheet of paper with the printed HSMFD hash to RKOS.		

Start the Terminal Session Logging

Step	Activity	Initials	Time
16	CA executes the command below using the terminal window to change the working directory to HSMFD: `cd /media/HSMFD`		
17	CA executes the command below to log activities of the **Commands** terminal window: `script script-20190814.log`		

Start the HSM Activity Logging

Step	Activity	Initials	Time

18	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
19	CA performs the following steps to prepare the HSM: a) Plug the null modem cable into the serial port of 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. **HSM3: Serial # H1403033** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Act 4. 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' cards
- 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 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 visible to everyone on the ceremony table. **CO1: Arbogast Fabian** **OP TEB # BB46592089** **SO TEB # BB46584451** **CO2: Dmitry Burkov** **OP TEB # BB46592090** **SO TEB # BB46584453** **CO5: Olafur Gudmundsson** **OP TEB # BB46592093** **SO TEB # BB46584666** **CO6: Nicolas Antoniello** **OP TEB # BB46592094** **SO TEB # BB46584459** **CO7: Subramanian Moonesamy** **OP TEB # BB46592106** **SO TEB # BB46584461**		

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 the cards that 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 2019 Q4

Step	Activity	Initials	Time
6	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[7] `/media/KSR/KSK38/ksr-root-2019-q4-0.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 Q4

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 2019 Q4, 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 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/KSK38/skr-root-2019-q4-0.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-201908*.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 the cards that 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.**		

Ceremony Break

Step	Activity	Initials	Time
16	CA divides the participants who desire a ceremony break into groups and ensures the following: a) Remaining participants are sufficient to maintain dual occupancy guidelines for the ceremony room. b) At least (2) Crypto Officers and (1) Auditor should remain in the ceremony room when each group is escorted for the ceremony break. c) Audit Cameras are never obstructed. RKOS will escort each group of participants out of the ceremony room for the ceremony break.		
17	Once all of the groups have returned to the ceremony room from the break, CA ensures that all participants are present and resumes the ceremony.		

Act 5. Issue Temporary CO, AAK, and SMK Cards

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

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

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

Issue Crypto Officer (CO) Cards

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

Issue Authorization Key (AAK) Cards

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

Issue Storage Master Key (SMK) Cards

Step	Activity	Initials	Time
4	CA performs the following steps to issue Storage Master Key (SMK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"4.SMK"**, press **ENT** to confirm. h) Select **"2.Backup SMK"**, press **ENT** to confirm. i) When **"Backup SMK?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"4"**, then press **ENT**. k) When **"Num Req Cards?"** is displayed, enter **"2"**, then press **ENT**. l) When **"Insert Card #X?"** is displayed, insert the required SMK card. m) When **"Remove Card?"** is displayed, remove the SMK card. n) Repeat steps l) to m) for the 2nd, 3rd and 4th SMK cards. o) When **"Verify Card #X?"** is displayed, insert the required SMK card. p) When **"Remove Card?"** is displayed, remove the SMK card. q) Repeat steps o) to p) for the 2nd, 3rd and 4th SMK cards. r) When **"SMK Backed Up"** is displayed, press **ENT** to confirm. s) Press **CLR twice** to return to the main menu **"Secured"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Act 6. KSK Deletion

The CA will delete the retired KSK from the HSM(s) by performing the steps below:

- List and identify the key(s) currently residing in the HSM
- Activate the HSM
- Remove the retired KSK from the HSM
- Verify the removal of the retired KSK is successful
- Remove the retired KSK from the App Key backup cards

List the KSK from the HSM

Step	Activity	Initials	Time
1	CA switches to the **HSM Output** terminal window.		

2	CA performs the following steps to list the KSK from 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**.
	    k) Press **CLR** to return to the menu **"Secured"**.
	
	Each card is returned to its designated card holder after use.
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

3	CA matches the displayed KSK label in the HSM Output terminal window. **KSK-2010: Kjqmt7v**		

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
4	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 the cards that 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.**		

Delete the KSK

Step	Activity	Initials	Time
5	CA switches to the **Commands** terminal window.		
6	CA list and matches the KSK by executing: **keybackup**[9] **–l –P 123456** **KSK-2010: Kjqmt7v**		
7	CA asks **"are there any objections?"** if not, CA deletes the KSK by executing: **keybackup**[9] **-d Kjqmt7v –P 123456**		
8	CA confirms that the **KSK-2010: Kjqmt7v** has been deleted by executing: **keybackup**[9] **–l –P 123456**		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
9	CA switches to the **HSM Output** terminal window.		
10	CA will switch to the **HSM Output** terminal window and press the **RESTART** button on HSM to make it Offline and wait for the Self Test to complete. Confirm the **"READY"** LED on the HSM is **OFF**.		

List the KSK from the HSM

Step	Activity	Initials	Time

11	CA performs the following steps to list the KSK from 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**.
	   k) Press **CLR** to return to the menu **"Secured"**.
	
	Each card is returned to its designated card holder after use.
	CA confirms that the **KSK-2010: Kjqmt7v** has been deleted
	
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

Return the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
12	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.**		
13	CA places the HSM into a prepared TEB, then seals it.		

14	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.
	
	HSM3: TEB # BB51184512 / Serial # H1403033		

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
15	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 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. 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 look for the HSM serial number. h) IW matches the displayed HSM serial number on the screen with the information below. **HSM4: TEB # BB51184671 / Serial # H1411006** **Last Verified: KSK36 2019-02-27** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

List and Delete the KSK from the HSM

Step	Activity	Initials	Time
16	CA performs the following steps to list the KSK from 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.**		
17	CA matches the displayed KSK label in the HSM Output terminal window. **KSK-2010: Kjqmt7v**		
18	CA performs the following steps to delete the KSK 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 **"2.Specify Key"**, press **ENT** to confirm. f) Select the **Kjqmt7v** key by pressing > to move it to the top of the HSM's display, then press **"A"** to select **Kjqmt7v**, then press < to see the key list. **Verify the (*) asterisk is next to Kjqmt7v** then 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.		
19	CA performs the following steps to list the KSK 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 the **KSK-2010: Kjqmt7v** has been deleted		

App Key Backups

Step	Activity	Initials	Time
20	CA performs the following steps to prepare the App key backups: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place the KSK on its designated area of the ceremony table. e) Give RKOS the backup HSMFDs. **KSK-2010: TEB # BB46584332** **Last Verified: KSK22 2015-08-13**		

Clear App Cards

Step	Activity	Initials	Time
21	CA will perform the following steps to clear App Key (KSK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"3.App Keys"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. h) Select **"5.Clear Media"**, press **ENT** to confirm. i) When **Clear Media?** is displayed, press **ENT** to confirm. j) Select **"2.Clear Card"**, press **ENT** to confirm. k) When **"Insert B/U Card ?"** is displayed, take the **App Key** card from the cardholder, show the **App Key** card to the audit camera and then insert the **App Key** card into the HSM's card reader. l) When **Card not empty Erase?** is displayed, press **ENT** to confirm. m) When **"Remove Card?"** is displayed, remove the App Key card. n) Repeat steps h) to m) for the 2nd App Key card. o) Press **CLR twice** to return to the main menu **"Secured"**. CA uses the shredder to destroy the cleared App Key cards. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Return the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
22	CA switches the HSM power to OFF, then disconnects the power and serial connections. **Note: DO NOT unplug the cable connections on the laptop.**		
23	CA places the HSM into a prepared TEB, then seals it.		
24	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 # BB51184513 / Serial # H1411006**		

Act 7. Introduce New HSM

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

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

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the new HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW 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. 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 look for the HSM serial number. h) IW matches the displayed HSM serial number on the screen with the information below. i) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **HSM5W: TEB # BB51184509 / Serial # H1903017** **Last Verified: AT38 2018-08-13** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Import the AAK

Step	Activity	Initials	Time

2	CA will perform the following steps to import the Adapter Authorization Key (AAK):
	
	    a) Utilize the HSM's keyboard to scroll through the menu using < >
	
	    b) Select **"2.Restore AAK"**, press **ENT** to confirm.
	
	    c) When **"Restore AAK?"** is displayed, press **ENT** to confirm.
	
	    d) When **"Insert Card #X?"** is displayed, insert the required AAK card.
	
	    e) When **"Remove Card?"** is displayed, remove the AAK card.
	
	    f) Repeat steps d) to e) for the 2nd AAK card.
	
	    g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm.
	
	Each card is returned to its designated card holder after use.
	Note: If the card is unreadable, gently wipe its metal contacts and try again.		

Configure the HSM to Secure State

Step	Activity	Initials	Time
3	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.Secure"**, press **ENT** to confirm. c) When **"Secure?"** is displayed, press **ENT** to confirm. d) When **"Insert Card SO #X?"** is displayed, insert the SO card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the SO card. g) Repeat steps d) to f) for the 2nd and 3rd SO cards. h) When **"SMK AES Triple DES?"** is displayed, press **CLR** to skip. i) When **"SMK AES"** is displayed, press **ENT** to confirm. j) When **"LAN Port Number?"** is displayed, press **CLR** to skip. k) When **"Enable IPv4/IPv6?"** is displayed, press **CLR** to skip. l) When **"LAN IPv4 Address?"** is displayed, press **CLR** to skip. m) When **"LAN IPv4 Mask?"** is displayed, press **CLR** to skip. n) When **"Set IPv4 Gateway?"** is displayed, press **CLR** to skip. o) When **"LAN IPv6 Address?"** is displayed, press **CLR** to skip. p) When **"LAN IPv6 Mask?"** is displayed, press **CLR** to skip. q) When **"Set IPv6 Gateway?"** is displayed, press **CLR** to skip. r) When **"Remote Mgmt Off Enable?"** is displayed, press **CLR** to skip. s) When **"Remote Mgmt Off** is displayed, press **ENT** to confirm. t) When **"Change Clock?"** is displayed, press **CLR** to skip. u) When **"Import Config?"** is displayed, press **CLR** to skip. v) When **"FIPS Mode On Disable?"** is displayed, press **CLR** to skip. w) When **"FIPS Mode On"** is displayed, press **ENT** to confirm. x) When **"Global Key Export Enabled"** is displayed, press **CLR** to skip. **Done Rebooting Device** will be displayed. IW records the cards that were used below. Each card is returned to its designated card holder after use. Set # _____ 1st SO card _____ of 7 2nd SO card _____ of 7 3rd SO card _____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Change the API Settings

Step	Activity	Initials	Time
4	CA performs the following steps to change the API settings: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"5. API Settings"**, press **ENT** to confirm. h) Select **"1.Key Import"**, press **ENT** to confirm. i) When **"Key Import On Disable?"** is displayed, press **ENT** to confirm. j) Select **"2.Key Export"**, press **ENT** to confirm. k) When **"Key Export On Disable?"** is displayed, press **ENT** to confirm. l) Select **"5.Sym Key Der"**, press **ENT** to confirm. m) When **"Sym Key Der On Disable?"** is displayed, press **ENT** to confirm. n) Press **CLR twice** to return to the main menu **"Secured"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Verify API Settings

Step	Activity	Initials	Time

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

App Key Backups

Step	Activity	Initials	Time
6	CA performs the following steps to prepare the App key backups: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place the KSK and the backup HSMFD on its designated area of the ceremony table. **KSK-2017: TEB # BB46584449** **Last Verified: KSK28 2017-02-02**		

Import the SMK and the KSK

Step	Activity	Initials	Time
7	CA will perform the following steps to import Storage Master Key (SMK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"4.SMK"**, press **ENT** to confirm. h) Select **"3.Restore SMK"**, press **ENT** to confirm. i) When **"Restore SMK?"** is displayed, press **ENT** to confirm. j) When **"Insert Card SMK #X?"** is displayed, insert the SMK card. k) When **"Remove Card?"** is displayed, remove the SMK card. l) Repeat steps j) to k) for the 2nd SMK card. m) When **"SMK Restored"** is displayed, press **ENT** to confirm. n) Press **CLR** to return to the main menu **"Key Mgmt"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
8	CA will perform the following steps to import KSK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required KSK card. g) When **"Remove Card?"** is displayed, remove the KSK card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR twice** to return to the main menu **"Secured"**. Card is returned to card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Return the KSK into a TEB

Step	Activity	Initials	Time
9	CA places the KSK and the backup HSMFD into a prepared TEB, then seals it.		
10	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the KSK TEB on the cart. **KSK-2017: TEB # BB46584387**		

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
11	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW records the cards that were used below. Each card is returned to its designated card holder after use. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
12	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		
13	CA performs the following steps to test the network connectivity between laptop and HSM: a) Use the **Commands** terminal window b) Test connectivity by executing: `ping hsm`[6] c) Wait for responses, then exit by pressing: `Ctrl + C`		

Insert Copy of the KSR FD

Step	Activity	Initials	Time
14	CA plugs the FD labeled **"KSR_COPY"** 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 Q4

Step	Activity	Initials	Time
15	CA executes the command below on the terminal window to sign the KSR file: **ksrsigner[7] /media/KSR_COPY/KSK38/ksr-root-2019-q4-0.xml**		
16	When the KSR signer displays the prompt: **Activate HSM prior to accepting in the affirmative!! (y/N):** CA confirms that the HSM is online, then enters **"y"** to proceed.		

Verify the KSR Hash for KSR 2019 Q4

Step	Activity	Initials	Time
17	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.		
18	Participants confirm that the hash displayed on the terminal window matches with the RZM readout, then CA asks **"are there any objections?"**		
19	CA enters **"y"** in response to **"Is this correct (y/N)?"** to complete the KSR signing operation. The SKR is located on: **/media/KSR_COPY/KSK38/skr-root-2019-q4-0.xml**		

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
20	CA executes the commands below using the terminal window to print the KSR Signer log: a) **lpadmin -p HP -o copies-default=X** **Note: Replace "X" with the amount of copies needed for the participants.** b) **printlog[8] $(ls -tr ksrsigner-201908*.log | tail -n 1)**		
21	IW attaches a copy of the required ksrsigner log to their script.		

Verification of the Hash of the SKR Copy

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

Remove Copy of the KSR FD

Step	Activity	Initials	Time

23	CA executes the following commands using the terminal window:
	　a) List the contents of the KSR FD by executing:
	　　`ls -ltrR /media/KSR_COPY`
	　b) Unmount the KSR FD by executing:
	　　`umount /media/KSR_COPY`		

24	CA removes the **KSR_COPY** containing the SKR files, then gives it to IW for audit purpose.		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
25	CA will switch to the **HSM Output** terminal window and press the **RESTART** button on HSM to make it Offline and wait for the Self Test to complete. Confirm the **"READY"** LED on the HSM is **OFF**.		

Clear and Destroy SMK Cards

Step	Activity	Initials	Time
26	CA will perform the following steps to clear Storage Master Key (SMK) cards: 　a) Utilize the HSM's keyboard to scroll through the menu using < > 　b) Select **"5.Key Mgmt"**, press **ENT** to confirm. 　c) When **"Insert CO Card #X?"** is displayed, insert the CO card. 　d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. 　e) When **"Remove Card?"** is displayed, remove the CO card. 　f) Repeat steps c) to e) for the 2nd CO card. 　g) Select **"4.SMK"**, press **ENT** to confirm. 　h) Select **"4.Clear Cards"**, press **ENT** to confirm. 　i) When **"Clear Card?"** is displayed, press **ENT** to confirm. 　j) When **"Insert Card SMK 1?"** is displayed, take the **SMK #1** card from the cardholder, show the **SMK #1** card to the audit camera and then insert the **SMK #1** card into the HSM's card reader. 　k) When **"Num Cards?"** is displayed, enter **"4"**, then press **ENT**. 　l) When **"Are you sure?"** is displayed, press **ENT** to confirm. 　m) When **"Remove Card?"** is displayed, remove the SMK card. 　n) When **"Insert Card SMK #X?"** is displayed, take the **SMK #X** card from the cardholder, show the **SMK #X** card to the audit camera and then insert the **SMK #X** card into the HSM's card reader. 　o) When **"Remove Card?"** is displayed, remove the SMK card. 　p) Repeat steps n) to o) for the 3rd and 4th SMK cards. 　q) Press **CLR twice** to return to the main menu **"Secured"**. CA uses the shredder to destroy the cleared SMK cards. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

Clear and Destroy CO and AAK Cards

Step	Activity	Initials	Time
27	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to clear Crypto Officer (CO) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"4.Clear RoleCard"**, press **ENT** to confirm. h) When **"Clear Card?"** is displayed, press **ENT** to confirm. i) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. j) When **"Insert Card #X?"** is displayed, take the required **CO #X** card from the cardholder, show the **CO #X** card to the audit camera and then insert the **CO #X** card into the HSM's card reader. k) When **"Are you sure?"** is displayed, press **ENT** to confirm. l) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. m) When **"Remove Card?"** is displayed, remove the CO card. n) Repeat steps j) to m) for the 2nd CO card. IW records the cards that were used below. Each card is returned to its designated card holder after use. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
28	CA performs the following steps to clear Adapter Authorization Key (AAK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Clear AAK Card"** from the same menu **"Role Mgmt"**, press **ENT** to confirm. c) When **"Clear AAK Card?"** is displayed, press **ENT** to confirm. d) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. e) When **"Insert Card AAK #X?"** is displayed, take the **AAK #X** card from the cardholder, show the **AAK #X** card to the audit camera and then insert the **AAK #X** card into the HSM's card reader. f) When **"Are you sure?"** is displayed, press **ENT** to confirm. g) When **"Remove Card?"** is displayed, remove the AAK card. h) Repeat steps e) to g) for the 2nd AAK card. i) Press **CLR** to return to the main menu **"Secured"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
29	CA uses the shredder to destroy the cleared CO an AAK cards.		

Act 8. Secure Hardware

The CA secures the ceremony hardware by performing the steps below:

- Backs up the HSMFD contents
- Prints log information
- Places the equipment and TCRs cards inside of TEBs
- Along with IW, escorts 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 power to OFF, then disconnects the power, serial, and ethernet connections. **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 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.
	
	HSM5W: TEB # BB51184514 / Serial # H1903017		

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 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`[4] `–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`[4] `–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-201908*.log` c) `enscript -Gr --font="Courier8" ttyaudit-tty*-201908*.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, and 1 sheet of 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 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 # BB46584386**		

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 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 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. **Laptop3: TEB # BB81420125 / Service Tag # C8SVSG2**		

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 card to the CO. h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. i) CO writes the date and time, then signs the table of IW's script, then IW initials the entry. j) Repeat steps for the 2 SO cards respectively, ensuring they're facing outward in the plastic case and placed into the prepared SO TEB. 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 # BB46584376** **SO TEB # BB46584377** **CO2: Dmitry Burkov** **OP TEB # BB46584378** **SO TEB # BB46584379** **CO5: Olafur Gudmundsson** **OP TEB # BB46584380** **SO TEB # BB46584381** **CO6: Nicolas Antoniello** **OP TEB # BB46584382** **SO TEB # BB46584383** **CO7: Subramanian Moonesamy** **OP TEB # BB46584384** **SO TEB # BB46584385**		

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	OP 1 of 7 SO 1 of 7	OP TEB # **BB46584376** SO TEB # **BB46584377**	**Arbogast Fabian**		**2019 Aug __**		
CO2	OP 2 of 7 SO 2 of 7	OP TEB # **BB46584378** SO TEB # **BB46584379**	**Dmitry Burkov**		**2019 Aug __**		
CO5	OP 5 of 7 SO 5 of 7	OP TEB # **BB46584380** SO TEB # **BB46584381**	**Olafur Gudmundsson**		**2019 Aug __**		
CO6	OP 6 of 7 SO 6 of 7	OP TEB # **BB46584382** SO TEB # **BB46584383**	**Nicolas Antoniello**		**2019 Aug __**		
CO7	OP 7 of 7 SO 7 of 7	OP TEB # **BB46584384** SO TEB # **BB46584385**	**Subramanian Moonesamy**		**2019 Aug __**		

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 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.**		
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. **HSM3: TEB # BB51184512** **HSM4: TEB # BB51184513** **HSM5W: TEB # BB51184514** **Laptop3: TEB # BB81420125** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386** **KSK-2017: TEB # BB46584387**		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
30	SSC1 writes the date and time, then signs 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 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
36	The COs return all credential TEBs to their respective safe deposit boxes by performing the steps below sequentially: a) CO reads aloud the TEB number(s), then verifies the 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. 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 # 1791** **OP TEB # BB46584376** **SO TEB # BB46584377** **CO2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46584378** **SO TEB # BB46584379** **CO5: Olafur Gudmundsson** **Box # 1789** **OP TEB # BB46584380** **SO TEB # BB46584381** **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584382** **SO TEB # BB46584383** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46584384** **SO TEB # BB46584385**		

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 and time, then signs 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 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.		
39	CA, IW, SSC2, and COs leave safe room closing the door behind them.		

Act 9. 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 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.		
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: **20190227 00:00:00 to 20190815 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 38**, 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*

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

---

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

Appendix B. Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

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

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: **Jonathan Denison**

Signature:

Date: 2019 Aug __

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: **20190227 00:00:00 to 20190815 00:00:00 UTC.**

SA:

_____

Signature:

_____

Date: 2019 Aug __

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 Aug __