Root DNSSEC KSK Ceremony 32

Wednesday February 7, 2018

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

This ceremony is executed under 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 found on https://www.iana.org/help/key-ceremony-roles

Instructions: At the end of the ceremony, participants sign on IW1's copy. IW1 records time upon completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN			
IW1	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO3	Joao Damas			
CO4	Carlos Martinez			
CO5	Olafur Gudmundsson			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Alejandro Bolivar / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Victor kao / RSM		___ February 2018	
AUD	Chris Koucheki / RSM			
SA1	Connor Barthold / ICANN			
SA2	Mike Brennan / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Jennifer Johnson / PTI			
SW	James Cole / ICANN			
SW	Audrey Fery-Forgues / ICANN			
EW	William Turton			
EW	Nathan Anderson			
EW	Matthew Justus			

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. Dual Occupancy is enforced. Only CAs, IWs, or SAs can enter and escort other participants to the Ceremony room. Only CA + IW can enter the safe room and escort other participants. CAs, IWs, or SAs may escort participants out of the ceremony room at the CA's discretion and only when an IW + CA or SA remain inside the ceremony. No one may leave the Ceremony room if the safe room is occupied. 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 and performs a roll call using the participants list on Page 2.		

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with 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.	IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room**:** Date and time: _____ 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 IW1 brings a flashlight then escorts SSC2, COs into the safe room.		
8.	SSC2 opens Safe #2 while shielding the combination from the camera.		
9.	SSC2 removes the existing safe log and shows the most recent page to the audit camera. SSC2 obtains the pre-printed safe log from IW1, then writes the date/time and signature on the safe log where “Open Safe” is indicated. IW1 verifies this entry, then initials it.		

COs Extract the Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	One by one, the selected CO retrieves the required OP TEB and SO TEB (if specified) by following the steps below a) With the assistance of the CA (and his/her common key), the CO opens her/his safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock** b) CO reads out the safe deposit box number, verifies its integrity, then removes his/her OP TEB and SO TEB c) CO reads out the TEB serial numbers, then verifies its integrity while showing it to the audit camera above. d) CO retains OP TEB and SO TEB (if specified below) then locks the box. e) CO writes the date/time and signature on the safe log where removal of their TEBs are indicated. f) IW1 verifies the completed safe log entries, then initials it. Repeat these steps until all required cards listed below are removed. **CO 1: Arbogast Fabian** **Box # 1791** OP TEB # **BB46584476 (Retain)** SO TEB # **BB46584451 (Check and Return)** **CO 2: Dmitry Burkov** **Box # 1793** OP TEB # **BB46584477 (Retain)** SO TEB # **BB46584453 (Check and Return)** **CO 3: Joao Damas** **Box # 1071** OP TEB # **BB46584454 (Retain)** SO TEB # **BB46584455 (Check and Return)** **CO 4: Carlos Martinez** **Box # 1068** OP TEB # **BB46584659 (Retain)** SO TEB # **BB46584665 (Check and Return)** **CO 5: Olafur Gudmundsson** **Box # 1789** OP TEB # **BB46584478 (Retain)** SO TEB # **BB46584666 (Check and Return)** **CO 6: Nicolas Antoniello** **Box # 1073** OP TEB # **BB46584479 (Retain)** SO TEB # **BB46584459 (Check and Return)** **CO 7: Subramanian Moonesamy** **Box # 1792** OP TEB # **BB46584480 (Retain)** SO TEB # **BB46584461 (Check and Return)**		

Close the Credential Safe #2

Step	Activity	Initials	Time
11.	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. IW1 verifies this 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 IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		
13.	IW1, CA, SSC2, and COs leave the safe room with smart card TEBs, closing the door behind them.		

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enter the safe room with a cart.		
15.	SSC1 opens Safe #1 while shielding the combination from the camera.		
16.	SSC1 takes out the existing safe log and shows the most recent page to the audit camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 writes the date/time and signature on the safe log where "Open Safe" is indicated. IW1 verifies this entry then initials it.		

Remove the Equipment from Safe #1

Step	Activity	Initials	Time
17.	CA extracts each equipment from the safe by following the steps below: a) CAREFULLY remove the equipment TEB from the safe. b) Read out the TEB serial number, then verify its integrity while showing it to the audit camera. c) Place 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) IW1 verifies the safe log entry, then initials it. HSM4: **TEB# BB51184612 / serial # H1411006 (Place on cart)** HSM3: **TEB# BB51184623 / serial # H1403033 (Check and Return)** Laptop1: **TEB# BB51184625 / serial # 37240147333 (Place on cart)** Laptop2: **TEB# BB24646591 / serial # 7292928457 (Check and Return)** OS DVD (release 20170403) + HSMFD: **TEB# BB46584481 (Place on cart)**		

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. IW1 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). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		
20.	CA, SSC1 and IW1 leaves the safe room with the cart, closing the door behind them.		

Act 2. Setup Equipment

Initial Setup

Step	Activity	Initials	Time
1.	CA prepares each equipment by following the steps below: a) Remove all equipment TEB from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read out the TEB # and the serial # (if applicable) while IW1 matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place it on its designated area on the ceremony table. HSM4: **TEB# BB51184612 / serial # H1411006** Laptop1: **TEB# BB51184625 / serial # 37240147333** OS DVD (release 20170403) + HSMFD: **TEB# BB46584481**		
2.	CA boots the laptop by following the steps below. a) Connect the power supply, external display, USB printer cable and USB null modem cable into the laptop. b) Immediately insert the new **OS DVD release 20170403** after the laptop power is switched ON.		
3.	CA sets up the laptop by following the steps below. a) Press "CTRL+ALT+F2" to get a console prompt and log in as **root**. b) Execute `system-config-display --noui` c) Execute `killall Xorg` d) Confirm that external display works. e) Log in as **root**		

Step	Activity	Initials	Time
4.	CA confirms that the printer is connected then configures printer as default and prints test page by going to **System > Administration > Printing** And follow the steps below: a) Click the **New Printer** icon (left side), leave everything default, then click the button **Forward.** b) Under "Select Connection" choose the first device "**HP Laserjet xxxx**" then click the button **Forward.** **Note**: The xxxx is the Printer Model c) Select **HP** and click the button **Forward.** d) Under "Models" scroll up and select **"Laserjet"** then click the button **Forward.** e) Click the button **Apply** to finish. f) Under "Local Printers" from the left menu, select "**printer".** g) Click the button **"Make Default Printer**" and "**Print Test Page".** h) Close the printer setup windows.		
5.	CA opens a terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal** Follow the additional steps to maximize the terminal window: a) Click the **View** menu and select **Zoom In.** b) Repeat the step above as necessary.		
6.	CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal window, CA executes: **`date -s "20180207 HH:MM:00"`** where **HH** is two-digit Hour, **MM** is two digit Minutes and **00** is Zero Seconds CA executes **`date`** using the Terminal window to confirm the date is properly configured.		

Format and label the blank FDs

Step	Activity	Initials	Time
7.	CA plugs a new FD into the laptop, then waits for it to be recognized by the OS, closes the file system popup window and formats the drive by executing **`df`** to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc), **`umount /dev/sda1`** to unmount the drive (change drive letter and partition if necessary), **`mkfs.vfat -n HSMFD -I /dev/sda1`** to execute a FAT32 format and label it as HSMFD. CA unplugs the FD.		
8.	CA repeats step 7 for the 2nd blank FD		
9.	CA repeats step 7 for the 3rd blank FD		
10.	CA repeats step 7 for the 4th blank FD		
11.	CA repeats step 7 for the 5th blank FD		

Connect the HSMFD

Step	Activity	Initials	Time
12.	CA plugs the **ceremony 30** HSMFD into the USB slot on the laptop and waits for the OS to recognize it. CA displays the HSMFD contents to all participants then closes the file system window. IW1 places the unused HSMFD 30 to the FD holder.		
13.	CA calculates the SHA-256 hash of the contents on the copied HSMFD by executing **`hsmfd-hash -c`** IW1 confirms that the result matches the SHA-256 hash of the HSMFD from the **Ceremony 30** annotated script. SHA-256 hash: 5f378217c62d0556dae2122c8dd32b89cf8d5167e4f9d3b512b79ab9bf2336c0 PGP Wordlist of the SHA-256 hash: PGP Words: eyetooth consensus miser bookseller southward clergyman adult escapade surmount tomorrow atlas Chicago optic sociable briefcase matchmaker stagehand microscope drunken graduate tonic Waterloo stapler positive atlas processor pupil proximate slingshot cannonball Christmas recipe **Note: CA will assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash from the ceremony script.**		

Start the Terminal Session Logging

Step	Activity	Initials	Time
14.	CA changes the default directory to the HSMFD by executing **`cd /media/HSMFD`**		
15.	CA executes **`script script-20180207.log`** to start a capture of terminal output.		

Start the HSM Output Logging

Step	Activity	Initials	Time
16.	CA opens a second terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal.** Follow the additional steps to maximize the terminal window: a) Click the **View** menu and select **Zoom In.** b) Repeat the step above as necessary. and executes **`cd /media/HSMFD`** and executes **`stty -F /dev/ttyUSB0 115200`** **`ttyaudit /dev/ttyUSB0`** to start logging HSM serial port outputs. Note: **DO NOT** unplug USB serial port from laptop as this causes logging to stop.		

Power Up the HSM

Step	Activity	Initials	Time
17.	CA prepares the HSM by following the steps below: a) Plug the ttyUSB0 null modem serial cable to the back of the HSM. b) Connect the power to HSM and switch the power ON. Status information should appear on the serial logging screen. c) Scroll the logging screen up for IW1 to match the displayed HSM serial number with the information below. **HSM4: serial # H1411006** **Note: The date/time on the HSM is not used as a reference for logging and timestamp.**		

Act 3. Activate HSM and Generate Signatures

Enable/Activate the HSM3

Step	Activity	Initials	Time
1.	One by one, CA calls each COs listed below to inspect the TEB for tamper evidence. With the help of the CA, the CO opens the TEB and hands the OP cards to the CA, then places it on the card holder visible to everyone. **CO 1: Arbogast Fabian** OP TEB # **BB46584476** **CO 2: Dmitry Burkov** OP TEB # **BB46584477** **CO 3: Joao Damas** OP TEB # **BB46584454** **CO 4: Carlos Martinez** OP TEB # **BB46584659** **CO 5: Olafur Gudmundsson** OP TEB # **BB46584478** **CO 6: Nicolas Antoniello** OP TEB # **BB46584479** **CO 7: Subramanian Moonesamy** OP TEB # **BB46584480**		
2.	CA activates the **HSM** by following the steps below: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, hit **ENT** to confirm. c) Insert the OP card, then hit **ENT** to confirm. d) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT.** e) When "**Remove Card?"** is displayed, remove the OP card. f) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW1 records the used cards below. Each card is returned to card holder after use. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7 **Note: If the smartcard is unreadable, gently wipe its metal contacts and try again.**		

Check the Network Connectivity Between Laptop and HSM4

Step	Activity	Initials	Time
3.	CA connects the HSM to the laptop using Ethernet cable in **LAN** port.		
4.	CA switches to the terminal window and tests network connectivity between laptop and HSM by executing: **`ping 192.168.0.2`** and wait for responses. Ctrl-C to exit program.		

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 four KSRs. One is for the normal operation and three are for fallback scenarios.		

Execute the KSR Signer for Phase D to E

Step	Activity	Initials	Time
6.	CA uses the terminal window to sign the KSR file by executing the following: **`ksrsigner /media/KSR/KSK32-0-D_to_E/ksr-root-2018-q2-0-d_to_e.xml`**		
7.	The KSR signer will provide the following 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

Step	Activity	Initials	Time
8.	When the program requests verification of the KSR hash, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room and provide documents for IW1 to review. b) RZM representative reads out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. c) IW1 retains the documents provided by the RZM representative and writes the name below: _____		
9.	Participants match the hash displayed on the terminal window, 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/KSK32-0-D_to_E/skr-root-2018-q2-0-d_to_e.xml`**		

Execute the KSR Signer for Phase E to D

Step	Activity	Initials	Time
11.	CA uses the terminal window to sign the KSR file by executing the following: **`ksrsigner /media/KSR/KSK32-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml`**		
12.	The KSR signer will provide the following 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

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 match the hash read out displayed on the terminal window. CA asks, "are there any objections"?		
15.	CA then enters **`"y"`** in response to **`"Is this correct y/n?"`** to complete the KSR signing operation. The SKR is located on **`/media/KSR/KSK32-1-E_to_D/skr-root-2018-q2-1-e_to_d.xml`**		

Execute the KSR Signer for Phase D to D

Step	Activity	Initials	Time
16.	CA uses the terminal window to sign the KSR file by executing the following: **`ksrsigner /media/KSR/KSK32-2-D_to_D/ksr-root-2018-q2-2-d_to_d.xml`**		
17.	The KSR signer will provide the following 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

Step	Activity	Initials	Time
18.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (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 match the hash read out displayed on the terminal window. 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 **`/media/KSR/KSK32-2-D_to_D/skr-root-2018-q2-2-d_to_d.xml`**		

Execute the KSR Signer for Phase C to C

Step	Activity	Initials	Time
21.	CA uses the terminal window to sign the KSR file by executing the following: **`ksrsigner /media/KSR/KSK32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml`**		
22.	The KSR signer will provide the following 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

Step	Activity	Initials	Time
23.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (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 match the hash read out displayed on the terminal window. 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 **`/media/KSR/KSK32-3-C_to_C/skr-root-2018-q2-3-c_to_c.xml`**		

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
26.	CA prints out sufficient number of copies for participants by executing the following command on the terminal window **`for i in $(ls -1 ksrsigner-20180207*.log); do printlog $i X; done`** **Note**: Replace **X** with the number of copies for the participants.		
27.	IW1 attaches a copy of each ksrsigner log to his/her script.		

Backup the Newly Created SKR

Step	Activity	Initials	Time
28.	CA copies the contents of the KSR FD by executing the following command on the terminal window **`cp –pR /media/KSR/* .`** Confirm overwrite by entering "y" if prompted.		
29.	CA uses the terminal window to perform the following commands: a) list the contents of the KSR FD by executing **`ls –ltrR /media/KSR`** b) flush the system buffers by executing **`sync`** c) unmount the KSR FD by executing **`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 cards to deactivate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Set Offline"**, then hit **ENT** to confirm. c) Insert the OP card, then hit **ENT** to confirm. d) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT.** e) When "**Remove Card?"** is displayed, remove the OP card. f) Repeat steps d) to e) for the 2nd and 3rd OP cards. Confirm that the **"READY"** LED on the HSM is **OFF.** IW1 records the used cards below. Each card is returned to card holder after use. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7 **Note: If the smartcard is unreadable, gently wipe its metal contacts and try again.**		

Test the Unused OP Card

Step	Activity	Initials	Time
32.	CA tests the unused OP card's readability by following the steps below: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"8.View Cards",** then hit **ENT** to confirm. c) Insert the OP card, then hit **ENT** to confirm. d) Verify that "OP" is displayed on the HSM, then hit **ENT** four times to display the information on the terminal window. e) Remove the OP card and return to the card holder. f) Hit **CLR** to return to the previous menu. IW1 records the used card below. OP card ____ of 7		

Act 4. Secure Hardware

Return the HSM to TEB

Step	Activity	Initials	Time
1.	CA switches the HSM to power OFF, then disconnects the power and laptop (serial and Ethernet) connections from it. **Note: DO NOT** unplug the connections on the laptop end.		
2.	CA places the HSM into a prepared TEB, then seals it.		
3.	CA performs the following steps: a) Read out the TEB# and HSM serial #, then shows it to the audit camera above for participants to see. b) Confirm with IW1 that the TEB# and HSM serial # match below. c) Initial the TEB with IW1 using a ballpoint pen. d) Give IW1 the sealing strips for later inventory. e) Place the HSM TEB on the cart. **HSM4: TEB# BB51184642 / serial # H1411006**		

Stop the Serial Port Activity and the Terminal Activity Logging

Step	Activity	Initials	Time
4.	CA performs the following steps to stop logging: a) Disconnect the USB serial adaptor from the laptop. b) Type "exit" then press enter on the Serial Port Activity (**ttyaudit**) window. c) Switch to the Terminal activity window. d) Type "exit" then press enter to stop logging. This window will remain open.		

Backup the HSMFD Contents

Step	Activity	Initials	Time
5.	CA sets dotglob by executing the command below on the terminal window **`shopt -s dotglob`** **Note:** This enables copying of all files from the original HSMFD.		
6.	CA prints two copies of the hash by executing the following command on the terminal window twice: **`hsmfd-hash -p`** **Note:** One copy for audit bundle and one copy for HSMFD package.		
7.	CA displays the contents of HSMFD by executing the following command on the terminal window **`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 HSMFD_		
9.	CA closes the file system window, then creates a backup of the HSMFD by executing following command on the terminal window **`cp -pR * /media/HSMFD_`**		
10.	CA displays the contents of HSMFD_ by executing the following command on the terminal window **`ls -ltrR /media/HSMFD_`**		
11.	CA matches the SHA-256 hash between the original HSMFD and the copy HSMFD by executing the following command on the terminal window **`hsmfd-hash -m`**		
12.	CA unmounts the HSMFD copy by executing the following command on the terminal window **`umount /media/HSMFD_`**		
13.	CA removes the **HSMFD_** and places it on the holder.		
14.	CA repeats step 8 to 13 for the 2nd copy.		
15.	CA repeats step 8 to 13 for the 3rd copy.		
16.	CA repeats step 8 to 13 for the 4th copy.		
17.	CA repeats step 8 to 13 for the 5th copy.		

Print Logging Information

Step	Activity	Initials	Time
18.	CA prints out a copy of the logging information by executing the following command on the terminal window **`enscript -2Gr -# 1 script-201802*.log`** **`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-201802*.log`** Attach the printed copies to IW1 script. **Note: Ignore the error regarding non-printable characters if prompted.**		

Place HSMFDs and OS DVDs into the TEB

Step	Activity	Initials	Time
19.	CA unmounts the HSMFD by executing the following commands on the terminal window **`cd /tmp`** **`umount /media/HSMFD`** CA removes the HSMFD, then places it on the holder.		
20.	CA performs the following steps to switch off the laptop: a) Turn off the laptop by pressing the power switch. b) Turn on the laptop by pressing the power switch and immediately remove the OS DVD from the laptop DVD drive. c) Disconnect all connections to the laptop including power, printer, display and network		
21.	CA places (2) HSMFD, (2) OS DVD, (1) paper with printed HSMFD hash inside the TEB, then seals it.		
22.	CA performs the following steps to verify the TEB: a) Read out the TEB#, then show it to the audit camera above for participants to see. b) Confirm with IW1 that the TEB# match below. c) Initial the TEB with IW1 using a ballpoint pen. d) Give IW1 the sealing strips for later inventory. e) Place the HSM TEB on the cart. OS DVD (release 20170403) + HSMFD: **TEB# BB46592049**		

Distribute the HSMFDs

Step	Activity	Initials	Time
23.	CA distributes the remaining HSMFDs: Two for IW1 (for audit bundles). Two for both RKOS (for SKR exchange with RZM and for process review).		

Return the Laptop to TEB

Step	Activity	Initials	Time
24.	CA places the laptop into a prepared TEB, then seals it.		
25.	CA performs the following steps: a) Read out the TEB# and Laptop serial #, then show it to the audit camera above for participants to see. b) Confirm with IW1 that the TEB# and Laptop serial # match below. c) Initial the TEB with IW1 using a ballpoint pen. d) Give IW1 the sealing strips for later inventory. e) Place the Laptop TEB on the cart. Laptop1 (Dell ATG6400): **TEB# BB51184640 / serial # 37240147333**		

Return the OP Cards to TEB

Step	Activity	Initials	Time
26.	One by one, CA calls each COs listed below 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 his/her 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 out the TEB # and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW1 keeps the sealing strips for later inventory. f) IW1 inspects the TEB, confirms the TEB # with the list below, then initials it with a ballpoint pen. g) CA gives the TEB containing the OP card to the CO. h) CO inspects the TEB, verifies its content, then initials it with a ballpoint pen. i) CO writes the date/time and signature on the table of IW1's script, then IW1 initials the entry. j) CO returns to his/her seat with the TEB and careful not to poke or puncture the TEB. k) Repeat steps for all the remaining COs on the list. **CO 1: Arbogast Fabian** OP TEB # **BB46592046** **CO 2: Dmitry Burkov** OP TEB # **BB46592047** **CO 3: Joao Damas** OP TEB # **BB46592048** **CO 4: Carlos Martinez** OP TEB # **BB46592050** **CO 5: Olafur Gudmundsson** OP TEB # **BB46592051** **CO 6: Nicolas Antoniello** OP TEB # **BB46592052** **CO 7: Subramanian Moonesamy** OP TEB # **BB46592053**		

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46592046	Arbogast Fabian		2018 February ____	UTC	
CO 2	OP 2 of 7	BB46592047	Dmitry Burkov		2018 February ____	UTC	
CO 3	OP 3 of 7	BB46592048	Joao Damas		2018 February ____	UTC	
CO 4	OP 4 of 7	BB46592050	Carlos Martinez		2018 February ____	UTC	
CO 5	OP 5 of 7	BB46592051	Olafur Gudmundsson		2018 February ____	UTC	
CO 6	OP 6 of 7	BB46592052	Nicolas Antoniello		2018 February ____	UTC	
CO 7	OP 7 of 7	BB46592053	Subramanian Moonesamy		2018 February ____	UTC	

Return the Equipment to Safe #1

Step	Activity	Initials	Time
27.	CA, IW1, SSC1 enters the safe room with the cart.		
28.	SSC1 opens Safe #1 while shielding the combination from the camera.		
29.	SSC1 removes the safe log and writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
30.	CA returns each equipment to the Safe by following the steps below: a) CAREFULLY remove the equipment TEB from the cart b) Read out the TEB # 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) IW1 verifies the safe log entry, then initials it. HSM4: **TEB# BB51184642 / serial # H1411006** Laptop1: **TEB# BB51184640 / serial # 37240147333** OS DVD (release 20170403) + HSMFD: **TEB# BB46592049**		

Close the Equipment Safe #1

Step	Activity	Initials	Time
31.	SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies this entry, then initials it.		
32.	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 IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		
33.	CA, SSC1 and IW1 leaves the safe room with the cart, closing the door behind them.		

Open the Credential Safe #2

Step	Activity	Initials	Time
34.	CA and IW1 brings a flashlight, then escorts SSC2, COs with their OP Card and SO Cards (if available) into the safe room.		
35.	SSC2 opens Safe #2 while shielding the combination from the camera.		
36.	SSC2 removes the safe log and writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies this entry, then initials it. **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
37.	One by one, the selected CO returns the TEBs of OP card by following the steps below. a) CO reads out their OP card TEB#, then verifies its integrity while showing it to the audit camera above b) With the assistance of the CA (and his/her common key), the CO opens his/her safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock** c) CO reads out the safe deposit box number, places his/her TEBs inside it, then locks it. d) CO writes the date/time and signature on the safe log "Return OP Card" is indicated. e) IW1 verifies the completed safe log entry, then initials it. Repeat these steps until all the required cards listed below are returned. **CO 1: Arbogast Fabian - Box # 1791** **OP TEB # BB46592046** **CO 2: Dmitry Burkov - Box # 1793** **OP TEB # BB46592047** **CO 3: Joao Damas - Box # 1071** **OP TEB # BB46592048** **CO 4: Carlos Martinez - Box # 1068** **OP TEB # BB46592050** **CO 5: Olafur Gudmundsson - Box # 1789** **OP TEB # BB46592051** **CO 6: Nicolas Antoniello - Box # 1073** **OP TEB # BB46592052** **CO 7: Subramanian Moonesamy - Box # 1792** **OP TEB # BB46592053**		

Close the Credential Safe #2

Step	Activity	Initials	Time
38.	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. IW1 verifies the safe log entry, then initials it.		
39.	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 IW1 verifies that the safe is locked and the "WAIT" light indicator is off.		
40.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.		

Act 5. Close the Key Signing Ceremony

Participants Signing of IW1'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 IW1's participants list. All signatures declare that this script is a true and accurate record of the ceremony.** IW1 records the completion time once all participants have signed the list.		
3.	CA reviews IW1's script and signs on the participants list.		
4.	CA acknowledges everyone's participation and notifies them that the Root DNSSEC KSK Signing Ceremony 32 has been completed. **Note: On-site participants that will not attend the HSM Destruction ceremony must sign out of the ceremony room log and will be escorted out of the facility.**		

Bundle Audit Materials

Step	Activity	Initials	Time
	IW1 makes (1) copy of his/her script for off-site audit bundle. Each Audit bundle contains: a) Output of signer system – HSMFD b) Copy of IW1's key ceremony script c) Audio-visual recording d) Logs from the Physical Access Control System and Intrusion Detection System (Range is **2017/08/17 – 2018/02/08**) e) IW1 attestation (Section A.1) f) SA1 attestation (Sections A.2 and A.3) All TEBs are labeled **"Root DNSSEC KSK Ceremony 32"**, dated and signed by **IW1 and CA**. Audit bundles are delivered to an off-site storage. **Note:** The CA holds the ultimate responsibility to finalize the audit bundle collection		

Audit Bundle Checklist:

1. Output of Signer System (CA)
One electronic copy (physical flash drive) of the HSMFD in each audit bundle. Each bundle is placed inside a TEB that is labeled, dated and signed by the CA and the IW1.

2. Key Ceremony Scripts (IW1)
Hard copies of the IW1's key ceremony scripts, including the IW1's notes and the IW1's attestation. See Appendix A.1.

3. Audio-visual recordings from the key ceremony (SA1)
One set is for the original audit bundle and another set as duplicate.

4. Logs from the Physical Access Control System (PACS) and Intrusion Detection System (IDS) (SA1)
Two electronic copies of the following:

a) Firewall configuration
b) Configuration Reports
c) Personnel/Cardholder Reports
d) Activity and Audit Log Reports

These files will be placed inside two separate Flash Drive labeled "Audit"
Each Flash Drives will be placed in the original audit bundle and duplicate audit bundle.
IW1 shall confirms the contents of the logs before placing the logs in the audit bundle.

5. Configuration review of the Physical Access Control System and Intrusion Detection System (SA1)
SA1's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix A.2.

6. Configuration review of the Firewall System (SA1)
SA1's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Other items
If applicable.

A.1 Key Ceremony Script (by IW1)

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.

Yuko Green

_____

Date: ___ February 2018

A.2 Access Control System Configuration Review (by SA1)

I have reviewed the access control system configuration, the assigned authorizations and the configuration audit log from the KMF. There were NO discrepancies found.

In generating reports, there were no filters applied on the interface that will limit the information displayed on the generated reports aside the date range specified below.

Enclosed are the following electronic copies from the access control system:

e) List of personnel with assigned access group.
f) Configurations for Areas and Access Groups.
g) Logs for Access Event Activities and Configuration Audit Activities.
(From the last log extraction **2017 August 17 00:00 UTC** to the date below)

Connor Barthold

_____

Date: ___ February 2018

A.3 Firewall Configuration Review (by SA1)

I have reviewed and determined that the firewall configuration satisfies the following requirements from the DNSSEC Practice Statement with version listed on the cover page.

1. No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communications network.
2. The Root Zone KSK Operator uses firewall to protect the production network from internal and external intrusion and to limit the nature and source of network activities that may access production systems that are related to key signing activities.

Connor Barthold

_____

Date: ___ February 2018