Root DNSSEC KSK Ceremony 29

Thursday April 27, 2017

Root Zone KSK Operator Key Management Facility
18155 Technology Drive, Culpeper, VA 22701-3805

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	**KSR =**	Key Signing Request	**OP =**	Operator
PTI =	Public Technical Identifiers	**RKOS =**	RZ KSK Operations Security	**RZM =**	Root Zone Maintainer
SA =	System Administrator	**SKR =**	Signed Key Response	**SO =**	Security Officer
SSC =	Safe Security Controller	**SW =**	Staff Witness		

TEB = Tamper Evident Bag (AMPAC, item #GCS1013,item #GCS0912 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large)

Participants

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

Title	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		___ April 2017	
IW1	Shauna Royston / ICANN			
SSC1	James Cole / ICANN			
SSC2	Derek Ellison / ICANN			
CO3	Olaf Kolkman / NL			
CO4	Robert Seastrom / US			
CO5	Christopher Griffiths / US			
CO6	Gaurab Upadhaya / NP			
CO7	Alain Aina / TG			
RZM	Alejandro Bolivar / Verisign			
RZM	Alex Brown / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Fonkam Teda / PricewaterhouseCoopers			
AUD	Eugene Jeong / PricewaterhouseCoopers			
SA1	Connor Barthold / ICANN			
SA2	Reed Quinn / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Matt Larson / ICANN			
SW	Kim Davies / PTI			
SW	LV McCoy / PTI			
EW	Dustin Phillips			
EW	Timothy McGinnis			
EW	Joseph Abley			
EW	Ashley Heineman			
EW	Sascha Sporschill			
EW	Anne Wang			

Note: <u>By signing this script, you are declaring that this is a true and accurate record of the Root DNSSEC KSK ceremony to the best of your knowledge.</u>

Note: Dual Occupancy is enforced. CA leads the ceremony. Only CAs, IWs, or SAs can enter the ceremony room and/or escort other participants. Only CA+IW can enter safe room and/or escort other participants. CAs, SAs or IWs may let individuals out of the ceremony room but only when CA+IW remain in the ceremony room. No one may leave when CA+IW are inside the safe room. Participants must sign in and out of the ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before the completion of the ceremony. The SA starts filming before the participants enter the room.

Some steps during the ceremony require the participants to tell and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the phonetic alphabet shown below will 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 Equipments

Participants Arrive and Sign into 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 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 Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 brings a flashlight then escorts SSC2, COs into the safe room.		
8.	SSC2, while shielding combination from camera, opens Safe #2.		
9.	SSC2 removes the existing safe log and shows the most recent page to the audit camera. IW1 provides a pre-printed safe log to the SSC2. SSC2 writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry then initials it.		

COs Extract 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 (as specified on the list below) by following the steps. 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 verifies the integrity of the safe deposit box, reads out its number, then removes his/her OP TEB and SO TEB c) CO reads out the TEB #s, then verifies its integrity. d) CO retains OP TEB and SO TEB (as specified below) then locks the box. e) CO writes date/time and signature on the safe log where the 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 3: Olaf Kolkman** **Box # 1239** OP TEB # **BB46584593 (Retain)** SO TEB # **BB46584594 (Check and Return)** **CO 4: Robert Seastrom** **Box # 1260** OP TEB # **BB46584595 (Retain)** SO TEB # **BB46584596 (Check and Return)** **CO 5: Christopher Griffiths** **Box # 1240** OP TEB # **BB46584597 (Retain)** SO TEB # **BB46584598 (Check and Return)** **CO 6: Gaurab Upadhaya** **Box # 1261** OP TEB # **BB46584298 (Retain)** SO TEB # **BB21907207 (Check and Return)** **CO 7: Alain Aina** **Box # 1242** OP TEB # **BB46584599 (Retain)** SO TEB # **BB46584600 (Check and Return)**		

Close 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 the safe log 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 safe room, with OP TEB and SO TEB (if applicable), closing the door behind them.		

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enter the safe room with an empty equipment cart.		
15.	SSC1, while shielding combination from camera, opens Safe #1.		
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 the safe log entry then initials it.		

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	**CA CAREFULLY removes HSM3 (in TEB)** from the safe; Reads out the TEB # and HSM serial # then places it on the equipment cart. CA then writes the date/time and signature on the safe log where HSM removal is indicated. IW1 verifies the safe log entry then initials it. **HSM3: TEB# BB24646656 / serial # H1403032** CA verifies the integrity of the other HSM that will not be used, then returns it in the safe. **HSM4: TEB# BB24646654 / serial # H1411011**		
18.	CA removes each of the following equipment TEBs from the safe, reads out the TEB # and serial # then places it on the equipment cart. CA then writes the date/time and signature on the safe log where the removed item(s) are indicated. IW1 verifies the safe log entry then initials it. **Laptop1 (Dell ATG6400): TEB# BB24646657 / serial # 41593712005** **OS DVD (release 20161014) + HSMFD: TEB# BB46584601** CA verifies the integrity of the other laptop that will not be used this time and return it to the safe. **Laptop2 (Dell ATG6400): TEB# BB24646655 / serial # 35063364997**		

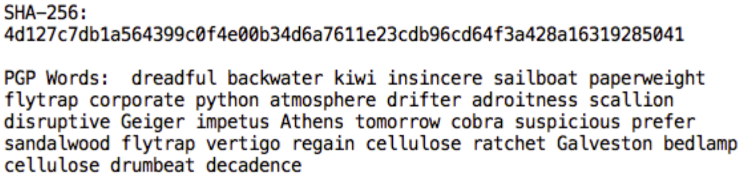
Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	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.		
20.	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.		
21.	CA, SSC1 and IW1 leaves the safe room with the equipment cart, closing the door behind them.		

Act 2. OS DVD Acceptance Test, Confirm and Sign the Key Signing Requests

OS DVD Acceptance Test

Step	Activity	Initials	Time
1.	CA inspects the laptop TEB for tamper evidence; reads out the TEB # and serial # while IW1 observes and matches it with the prior ceremony script in this facility. CA then places the laptop on the key ceremony table. **Laptop1 (Dell ATG6400): TEB# BB24646657 / serial # 41593712005**		
2.	CA inspects the OS DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it with the prior ceremony script in this facility. CA then places the items on the key ceremony table. **OS DVD (release 20161014) + HSMFD: TEB# BB46584601**		
3.	CA removes and discards the TEB from the laptop, OS DVD + HSMFD, then connects the laptop power, external display, general purpose external DVD drive. CA then boots the laptop from **OS DVD (release 20161014).**		
4.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes `system-config-display --noui` c) CA executes `killall Xorg` d) CA confirms that external display works. e) CA logs in as root		
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		

Step	Activity	Initials	Time
6.	CA inserts the new OS DVD **release 20170403** into the external DVD drive, waits for it to be recognized by the OS and performs the following: a) Close the file system popup window b) Confirm the assigned drive letter by executing **`df`** c) Unmount the DVD drive by executing **`umount /dev/scd1`** d) Calculate the SHA-256 hash by executing **`sha2wordlist < /dev/scd1`** IW1 and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash. **Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash written on the ceremony script.**  SHA-256: 4d127c7db1a564399c0f4e00b34d6a7611e23cdb96cd64f3a428a16319285041 PGP Words: dreadful backwater kiwi insincere sailboat paperweight flytrap corporate python atmosphere drifter adroitness scallion disruptive Geiger impetus Athens tomorrow cobra suspicious prefer sandalwood flytrap vertigo regain cellulose ratchet Galveston bedlamp cellulose drumbeat decadence **Note: The SHA-256 hash of the OS DVD is also published on the IANA website** **https://data.iana.org/ksk-ceremony/29/KC-20170403.iso.sha256**		
7.	CA removes the OS DVD by pressing the eject button on the external DVD drive, then places it on the ceremony table, having it visible to the audit camera and the participants.		
8.	CA repeats step 6 and 7 for the 2nd copy of the new OS DVD **release 20170403**.		
9.	IW1 records the date, time then affixes his/her signature upon successful completion of the OS DVD release **20170403** acceptance testing: **OS DVD Acceptance Test release 20170403** **Printed Name** **Shauna Royston** **Date** **2017/04/27** **Time** ______________________________ **Signature** ______________________________		
10.	CA disconnects the general purpose external DVD drive from the laptop, then removes the OS DVD by performing: a) Turn off the laptop by pressing the power switch b) Turn on the laptop by pressing the power switch and immediately remove the old OS DVD **(release 20161014)** from the laptop DVD drive c) Disconnect the laptop to power off		
11.	CA discards all the old OS DVD **(release 20161014)** copies.		

Set Up Laptop

Step	Activity	Initials	Time
12.	CA connects the laptop power, printer and boots the laptop using the new **OS DVD release 20170403**.		
13.	CA sets up the laptop by following the steps below. a) CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root. b) CA executes **`system-config-display --noui`** c) CA executes **`killall Xorg`** d) CA confirms that external display works. e) CA logs in as root		
14.	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 and then click the button **Forward** b) Under "Select Connection" choose the first device "**HP Laserjet xxxx**" and 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"**, and 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		
15.	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: c) Click the **View** menu and select **Zoom In** d) Repeat the step above as necessary		
16.	CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal window, CA executes: **`date -s "20170427 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.		

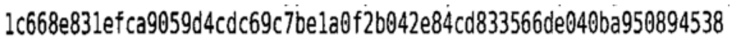
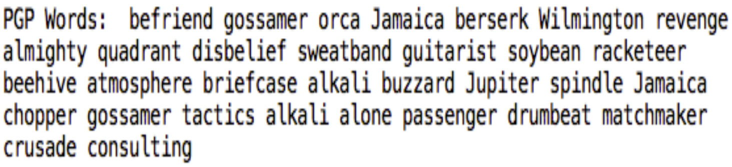
Format and label blank FD

Step	Activity	Initials	Time

17.	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.		

18.	CA repeats step 17 for the 2nd blank FD		
19.	CA repeats step 17 for the 3rd blank FD		
20.	CA repeats step 17 for the 4th blank FD		
21.	CA repeats step 17 for the 5th blank FD		

Connect HSMFD

Step	Activity	Initials	Time
22.	CA plugs the previous HSMFD used in the **ceremony 27** into the free USB slot on the laptop and waits for OS to recognize it. CA displays the HSMFD contents to all participants then closes the file system window.		
23.	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 27** annotated script (image from Ceremony 27 annotated script). SHA-256 hash:  1c668e831efca9059d4cdc69c7be1a0f2b042e84cd833566de040ba950894538 PGP Wordlist of the SHA-256 hash:  PGP Words: befriend gossamer orca Jamaica berserk Wilmington revenge almighty quadrant disbelief sweatband guitarist soybean racketeer beehive atmosphere briefcase alkali buzzard Jupiter spindle Jamaica chopper gossamer tactics alkali alone passenger drumbeat matchmaker crusade consulting **Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash written on the ceremony script.**		

Start Logging Terminal Session

Step	Activity	Initials	Time
24.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`		
25.	CA executes `script script-20170427.log` to start a capture of terminal output.		

Start Logging HSM Output

Step	Activity	Initials	Time
26.	CA connects a serial to USB null modem cable to laptop.		

27.	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 HSM

Step	Activity	Initials	Time
28.	CA inspects the HSM TEB for tamper evidence; reads out the TEB # and HSM serial # while IW1 observes and matches it with the prior ceremony script in this facility. **HSM3: TEB# BB24646656 / serial # H1403032**		
29.	CA removes and discards the TEB of the HSM, then plugs ttyUSB0 null modem serial cable to the back of the HSM.		
30.	CA switches to the ttyaudit terminal window and connects power to HSM and switches the power ON. Status information should appear on the serial logging screen. IW1 matches the displayed HSM serial number with below. **HSM3: serial # H1403032** **Note: The date/time on the HSM is not used as a reference for logging and timestamp.**		

Enable/Activate HSM3

Step	Activity	Initials	Time
31.	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 cardholder visible to everyone. **CO 3: Olaf Kolkman** OP TEB # **BB46584593** **CO 4: Robert Seastrom** OP TEB # **BB46584595** **CO 5: Christopher Griffiths** OP TEB # **BB46584597** **CO 6: Gaurab Upadhaya** OP TEB # **BB46584298** **CO 7: Alain Aina** OP TEB # **BB46584599**		
32.	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",** then hit **ENT** to confirm c) When **"Set Online?"** is displayed, then hit **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT** f) When "**Remove Card?"** is displayed, then remove the card g) 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 cardholder after use. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7		

Check Network Connectivity Between Laptop and HSM3

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

Insert Copy of KSR to be Signed

Step	Activity	Initials	Time
35.	The KSR FD was transferred to the facility by the RKOS. It contains three KSRs. One is for the normal operation and two are for fallback scenarios. 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.		

Execute KSR Signer for Phase C to D

Step	Activity	Initials	Time
36.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK29-0-C_to_D/ksr-root-2017-q3-0-c_to_d.xml`		
37.	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.		

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
38.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room. The RZM provides identification document for the IW1 to review and retain. RZM, then reads out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. IW1 enters the RZM representative’s name here: ______________________________________		
39.	Participants match the hash read out displayed on the terminal window. CA asks, “are there any objections”?		
40.	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/KSK29-0-C_to_D/skr-root-2017-q3-0-c_to_d.xml`		

Execute KSR Signer for Phase D to C

Step	Activity	Initials	Time
41.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK29-1-D_to_C/ksr-root-2017-q3-1-d_to_c.xml`		
42.	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.		

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
43.	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.		
44.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?		
45.	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/KSK29-1-D_to_C/skr-root-2017-q3-1-d_to_c.xml`		

Execute KSR Signer for Phase C to C

Step	Activity	Initials	Time
46.	CA uses the terminal window to sign the KSR file by executing the following: **`ksrsigner /media/KSR/KSK29-2-C_to_C/ksr-root-2017-q3-2-C_to_c.xml`**		
47.	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.		

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initials	Time
48.	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.		
49.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?		
50.	CA enters "**`y`**" in response to "**`Is this correct y/n?`**" to complete the KSR signing operation. The SKR is located on **`/media/KSR/KSK29-2-C_to_C/skr-root-2017-q3-2-c_to_c.xml`**		

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
51.	CA prints out sufficient number of copies for participants by executing the following command on the terminal window **`for i in $(ls -1 ksrsigner-20170427-*.log); do printlog $i X; done`** **Note**: Replace **X** with the number of copies for the participants.		
52.	IW1 attaches a copy of each ksrsigner log to his/her script.		

Backup Newly Created SKR

Step	Activity	Initials	Time
53.	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” when prompted.		
54.	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`**		
55.	CA removes the **KSR** FD containing the SKR files, then gives it to the RZM representative.		

Disable/Deactivate HSM

Step	Activity	Initials	Time
56.	CA ensures to utilize the cards that were NOT used on the prior steps. CA will perform the following steps 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) When **“Set Offline?”** is displayed, then hit **ENT** to confirm d) When **“Insert Card OP #?”** is displayed, insert the OP card from the cardholder e) When **“PIN?”** is displayed, enter **“11223344”,** then hit **ENT** f) When **“Remove Card?”** is displayed, then remove the card g) Repeat steps d) to f) for the 2nd and 3rd OP cards Confirm the **“READY”** LED on the HSM is **OFF.** IW1 records the used cards below. Each card is returned to cardholder after use. 1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7		

Act 3. Secure Hardware and Close the Ceremony

Return 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. **Note: DO NOT unplug the connections on the laptop end.**		
2.	CA places the HSM into a prepared TEB, then seals it.		
3.	CA reads out the TEB # and the HSM serial #, then shows it to the participants. IW1 confirms the TEB # and HSM serial # below. **HSM3: TEB# BB51184621 / serial # H1403032** CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory. CA places the HSM TEB on the equipment cart.		

Stop Recording Serial Port Activity and Logging Terminal Output

Step	Activity	Initials	Time
4.	**Closing ttyaudit terminal window** CA terminates the HSM serial output capture by disconnecting the USB serial adaptor from the laptop. CA then exits out of Serial Port Activity **(ttyaudit) terminal window** by typing “exit”, then press enter.		
5.	**Terminating the logging script** CA stops the logging terminal output by typing “exit”, then press enter. **Note:** This only stops the script logging and will **NOT** close the terminal window.		

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA sets dotglob by executing the following command on the terminal window `shopt -s dotglob` **Note:** This enables copying of all files from the original HSMFD.		
7.	CA prints two copies of the hash by executing the following command on the terminal window `for i in $(seq 2); do hsmfd-hash -p; done` **Note:** One copy for audit bundle and one copy for HSMFD package.		
8.	CA displays contents of HSMFD by executing the following command on the terminal window `ls -ltrR`		
9.	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_ CA closes the file system window and 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 9 to 12 for the 2nd copy.		
15.	CA repeats step 9 to 12 for the 3rd copy.		
16.	CA repeats step 9 to 12 for the 4th copy.		
17.	CA repeats step 9 to 12 for the 5th copy.		

Print Logging Information

Step	Activity	Initials	Time

18.	CA prints out a hard copy of the logging information by executing the following command on the terminal window
	`enscript -2Gr -# 1 script-20170427.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20170427-*.log`
	for attachment to IW1 script.
	Note: Ignore the error regarding non-printable characters if prompted.		

Place HSMFD and OS DVD 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 turn 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 removes the OS DVD from the laptop DVD drive. c) Disconnect power from the laptop.		
21.	CA places **(2)** HSMFDs, **(2)** OS DVD and **(1)** paper with printed HSMFD hash into a prepared TEB, then seals it. CA reads out the TEB #, then shows it to IW1 and participants to confirms. **OS DVD (release 20170403) + HSMFD: TEB# BB46584512**		
22.	CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory. CA places the OS DVD and HSMFD TEB on the equipment cart.		

Distribute 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)		

Returning Laptop to TEB

Step	Activity	Initials	Time
24.	CA disconnects all connections to the laptop including printer, display and network, then places it into a prepared TEB, then seals it. CA reads out the TEB #, then shows it to IW1 and participants to confirm. **Laptop1 (Dell ATG6400): TEB# BB51184616 / serial # 41593712005**		
25.	CA and IW1 initials the TEB using a ballpoint pen, then IW1 keeps the sealing strips for later inventory. CA places the laptop TEB on the equipment cart.		

Return OP Card 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 OP TEB and plastic case prepared for the CO. b) CO takes his/her OP card from the cardholder 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 and 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 and 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 3: Olaf Kolkman** **OP TEB # BB46584464** **CO 4: Robert Seastrom** **OP TEB # BB46584465** **CO 5: Christopher Griffiths** **OP TEB # BB46584466** **CO 6: Gaurab Upadhaya** **OP TEB # BB46584467** **CO 7: Alain Aina** **OP TEB # BB46584468**		

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 3	OP 3 of 7	BB46584464	Olaf Kolkman		___ April 2017	UTC	
CO 4	OP 4 of 7	BB46584465	Robert Seastrom		___ April 2017	UTC	
CO 5	OP 5 of 7	BB46584466	Christopher Griffiths		___ April 2017	UTC	
CO 6	OP 6 of 7	BB46584467	Gaurab Upadhaya		___ April 2017	UTC	
CO 7	OP 7 of 7	BB46584468	Alain Aina		___ April 2017	UTC	

Returning Equipment to Safe #1

Step	Activity	Initials	Time
27.	CA, IW1, SSC1 enters the safe room with the equipment cart.		
28.	SSC1, while shielding the combination from the camera, opens Safe #1.		
29.	SSC1 removes the safe log and writes the date/time and signature on the safe log where the Open Safe is indicated. IW1 verifies the safe log entry and then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
30.	CA **CAREFULLY** removes the HSM TEB from the cart, reads out the TEB # and the HSM serial #, then **CAREFULLY** places it inside Safe #1. CA writes the date/time and signature on the safe log where "HSM return" is indicated. IW1 verifies the safe log entry and initials it. **HSM3: TEB# BB51184621 / serial # H1403032**		
31.	CA removes each of the following TEBs from the equipment cart; reads out the TEB # and serial # (if applicable), then places it inside the Safe #1. CA writes the date/time and signature on the safe log where the returned item is indicated. IW1 verifies the safe log entry and initials it. **Laptop1 (Dell ATG6400): TEB# BB51184616 / serial # 41593712005** **OS DVD (release 20170403) + HSMFD: TEB# BB46584512**		

Close Equipment Safe #1

Step	Activity	Initials	Time
32.	SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry and then initials it.		
33.	SSC1 returns the safe log back to 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.		
34.	CA, SSC1 and IW1 leaves the safe room with the equipment cart closing the door behind them.		

Open Credential Safe #2

Step	Activity	Initials	Time
35.	CA and IW1 brings a flashlight, then escorts SSC2, COs with their OP Card and SO Cards (if available) in TEBs into the safe room.		
36.	SSC2, while shielding combination from the camera, opens Safe #2.		
37.	SSC2 removes the safe log and writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies the safe log entry and then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
38.	One by one, the selected CO returns the TEBs of OP and SO cards (as specified on the list below) by following the steps below. a) CO reads out their OP card TEB # and SO card TEB # (as specified on the list) and verifies its integrity 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, verifies its integrity, places his/her TEBs inside it and then locks it. d) CO writes the date/time and signature on the safe log that indicates return of the cards. e) IW1 verifies the completed safe log entries and then initials it. Repeat these steps until all the required cards listed below are returned. **CO 3: Olaf Kolkman** **Box # 1239** **OP TEB # BB46584464** **CO 4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584465** **CO 5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46584466** **CO 6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB46584467** **CO 7: Alain Aina** **Box # 1242** **OP TEB # BB46584468**		

Close Credential Safe #2

Step	Activity	Initials	Time
39.	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 and then initials it.		
40.	SSC2 returns the safe log back to Safe #2 and 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.		
41.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.		

Participant Signing of IW1's Script

Step	Activity	Initials	Time
42.	CA reads the exceptions that may have occurred during the ceremony.		
43.	CA calls each attendee on the participants list to proceed to the ceremony table to confirm their printed name and date. Each attendee will **sign IW1's participants list declaring that this script is a true and accurate record of the ceremony.** IW1 records the completion time once all participants have signed the participants list.		
44.	CA reviews IW1's script and signs the participants list.		

Stop Online Streaming

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

Sign Out of Ceremony Room

Step	Activity	Initials	Time
46.	RKOS ensures that all participants sign out of the Ceremony Room log and are then escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.		

Stop Video Recording

Step	Activity	Initials	Time
47.	CA notifies the SA to stop video recording.		

Bundle Audit Materials

Step	Activity	Initials	Time
48.	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 **10/27/2016 – 04/27/2017**) e) IW1 attestation (Section A.1) f) SA attestation (Sections A.2 and A.3) All TEBs are labeled **"Root DNSSEC KSK Ceremony 29"**, dated and signed by **IW1 and CA**. An off-site audit bundle is delivered to an off-site storage. **The CA holds the ultimate responsibility to finalize the audit bundle collection**		

All remaining participants sign out of ceremony room log and leave.

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 tamper-evident bag 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 the other as a duplicate.

4. Logs from the Physical Access Control System (PACS) and Intrusion Detection System (IDS) (SA1)
One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PACS and IDS configuration review, the list of enrolled users, the event log and configuration audit log files are contained in each audit bundle. Each audit bundle is placed in a tamper-evident bag that is labeled, dated and signed by the SA1 and the IW1.

IW1 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 with this script and any exceptions that may have occurred were accurately and properly documented.

Shauna Royston

____

Date: ___ April 2017

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

I have reviewed the access control system configuration, the configuration audit log and the assigned authorizations from the other KMF and not found any discrepancies or anything else out of the ordinary.

Enclosed are the configuration audit log, the list of assigned authorizations and the screenshots of the roles configurations.

Enclosed is also an electronic copy of the event log from the access control system ranging from the last log extraction on **27 October 2016 00:00 UTC** to now.

Connor Barthold

____

Date: ___ April 2016

A.3 Firewall Configuration Review (by SA1)

I have reviewed the firewall configuration from the other KMF and not found any discrepancies or anything else out of the ordinary.

Enclosed is the configuration extract from the firewall unit.

Connor Barthold

____

Date: ___ April 2016