Root DNSSEC KSK Ceremony 28

Thursday February 2, 2017

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	**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	Richard Lamb / ICANN			
IW1	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian / TZ			
CO2	Dmitri Burkov / RU			
CO3	Joao Damas / PT			
CO4	Carlos Martinez / UY			
CO6	Nicolas Antoniello / UY			
CO7	Subramanian Moonesamy / MU			
RZM	Alejandro Bolivar / Verisign			
RZM	John Painumkal / Verisign			
AUD	Ken Michaels / PwC			
AUD	Rafael Menchaca / PwC			
SA1	Connor Barthold / ICANN			
SA2	Josh Jenkins / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
CA3	Kim Davies / PTI			
SW	Alain Durand / ICANN			
SW	Dennis Chang / ICANN			
SW	Steve Conte / ICANN			
SW	James Cole / ICANN			
EW	Andrew Pfeifer / Mel Films			
EW	Mor Albalak / Mel Films			
EW	David Freid / Mel Films			

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 Equipment

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 list of participants 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 electronics 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 and SO TEBs 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 removes his/her OP TEB and SO TEB; verifies the integrity of the safe deposit box and reads out the box number then locks it. c) CO reads out the TEB #s and verifies the integrity of his/her OP and SO Cards d) CO writes date/time and signature on the safe log where the removal of his/her OP and SO cards are indicated. Repeat these steps until all required cards listed below are removed. IW1 verifies the completed safe log entries then initials it. **CO 1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46584657 (Retain)** **SO TEB # BB46584663 (Retain)** **CO 2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46584658 (Retain)** **SO TEB # BB46584652 (Retain)** **CO 3: Joao Damas** **Box # 1071** **OP TEB # BB46584281 (Retain)** **SO TEB # BB21820433 (Retain)** **CO 4: Carlos Martinez** **Box # 1068** **OP TEB # BB46584659 (Retain)** **SO TEB # BB46584665 (Retain)** **CO 6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584661 (Retain)** **SO TEB # BB46584667 (Retain)** **CO 7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46584662 (Retain)** **SO TEB # BB46584668 (Retain)**		

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 log back in the Safe 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 OP and SO TEBs, closing the door behind them.		

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enters the safe room with an empty equipment cart.		
15.	SSC1, while shielding combination from camera, opens the 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 each of the following HSM TEBs 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# BB24646618 / serial # H1403033** **HSM4: TEB# BB24646625 / serial # H1411006**		
18.	CA removes each of the following equipment TEBs from the safe, reads out the TEB # and serial # (if applicable) 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: TEB# BB24646622 / serial # 37240147333** **OS DVD (release 20160503) + HSMFD: TEB# BB46584720** **APP Key KSK-2017: TEB# BB46584642** **APP Key KSK-2017: TEB# BB46584643** Verify the integrity of the other Laptop that will not be used during this ceremony, then return it to the safe. **Laptop2: TEB# BB24646591 / serial # 7292928457**		

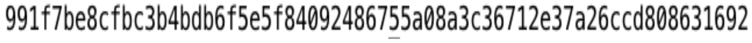
Close Equipment Safe #1 and exit safe room

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 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: TEB# BB24646622 / serial # 37240147333**		
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 20160503) + HSMFD: TEB# BB46584720**		
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 20160503).**		
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 20161014** into the external DVD drive, waits for it to be recognized by the OS, then 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 SHA256 hash by executing **`sha256sum /dev/scd1`** **`SHA256 hash for release 20161014:`** 991f7be8cfbc3b4bdb6f5e5f84092486755a08a3c36712e37a26ccd808631692 IW1 and participants confirm that the result matches the above, which also matches the one published on: https://data.iana.org/ksk-ceremony/27/KC-20161014.iso.sha256		
7.	CA removes the OS DVD by pressing the eject button on the external DVD drive and places it on the ceremony table visible from the audit camera and the participants.		
8.	CA repeats step 6 and 7 for the 2nd copy of the new OS DVD **release 20161014**.		
9.	IW1 records the date, time then writes his/her signature upon successful completion of the OS DVD release 20161014 acceptance testing: **OS DVD Acceptance Test release 20161014** **Printed Name** **Yuko Green** **Date** **2017/02/02** **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 20160503)** from the laptop DVD drive c) Disconnect the laptop power to power off the laptop		
11.	CA discards the old OS DVD **(release 20160503)** copies.		

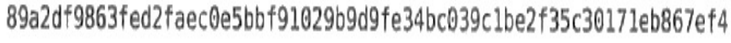
Set Up Laptop

Step	Activity	Initials	Time
12.	CA connects the laptop power, printer and Ethernet cable and boots the laptop using the new **OS DVD release 20161014**.		
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 by following 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 windows, CA executes: **`cp /usr/share/zoneinfo/UTC /etc/localtime`** When **“``cp: overwrite `/etc/localtime’?``”** is displayed, type **“`y`”** and press enter. Then, CA executes **`date -s “20170202 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, waits for it to be recognized by the OS, closes the file system popup window, then 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 number if necessary) **`mkfs.vfat -n HSMFD -I /dev/sda1`** to execute a FAT32 format and label it as HSMFD. then, 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		
22.	CA repeats step 17 for the 6th blank FD		

Connect HSMFD

Step	Activity	Initials	Time
23.	CA plugs the **ceremony 26** HSMFD into the free 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.		
24.	Calculate the sha256 hash of the contents on the copied HSMFD. **`find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum`** IW1 confirms that the result matches the sha256 hash of the HSMFD from the **Ceremony 26** annotated script. (image from Ceremony 26 annotated script).  89a2df9863fed2faec0e5bbf91029b9d9fe34bc039c1be2f35c30171eb867ef4 **Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the others confirm the hash written on this ceremony script.**		

Start Logging Terminal Session

Step	Activity	Initials	Time
25.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`		
26.	CA executes `script script-20170202.log` to start a capture of terminal output.		

Start Logging HSM Output

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

28.	CA opens a second terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal.**
	Follow the additional steps below 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 HSM3

Step	Activity	Initials	Time
29.	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# BB24646618 / serial # H1403033**		
30.	CA removes and discards the TEB from the HSM, then plugs ttyUSB0 null modem serial cable and Ethernet cable in **LAN** port.		
31.	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 # H1403033** **Note: The date/time on the HSM is not used as a reference for logging and timestamp.**		

Enable/Activate HSM3

Step	Activity	Initials	Time
32.	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 1: Arbogast Fabian** **OP TEB # BB46584657** **CO 2: Dmitry Burkov** **OP TEB # BB46584658** **CO 3: Joao Damas** **OP TEB # BB46584281** **CO 4: Carlos Martinez** **OP TEB # BB46584659** **CO 6: Nicolas Antoniello** **OP TEB # BB46584661** **CO 7: Subramanian Moonesamy** **OP TEB # BB46584662**		
33.	CA activates the HSM by following the steps below: a) Utilize the HSM's keyboard and scroll through the menu using <> key b) Select **"1.Set Online"** press **ENT** to confirm c) When **"Set Online?"** is displayed, press **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card 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
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 KSRs are downloaded to the KSR FD and transferred to the facility by the RKOS. CA plugs FD labeled **"KSR"** to be signed into the laptop and waits for the OS to recognize the FD. CA points out the KSR file to be signed then closes the file system window.		

Execute KSR signer

Step	Activity	Initials	Time
36.	CA identifies the KSR to be signed and executes, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2017-q2-0.xml`		
37.	The KSR signer will ask whether the HSM is activated or not as below. `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters "y" to proceed to verification. Note: DO NOT enter " y" for the " Is this correct y/n?" yet.		

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 a representative from the Root Zone Maintainer (RZM) to identify him/herself. The RZM representative provides identification document(s) for IW1 to verify and retain. IW1 enters the RZM representative's name below: ______________________________		
39.	CA requests for participants to match the displayed hash while RZM representative reads out the SHA256 hash in PGP wordlist format to confirm the KSR sent to the Root Zone KSK Operator. CA asks, "are there any objections"?		
40.	CA then enters **"y"** in response to **"Is this correct y/n?"** to complete KSR signing operation. Output should look like sample Figure 1. The signed KSR (SKR) file is in: `/media/KSR/skr-root-2017-q2-0.xml`		

```
$ ksrsigner Kjqmt7v ksr-root-2010-q4-1.xml

Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2010-q4-1.xml (at Mon Jul 12 22:44:26 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper Pro 0405
    Serial:          K6002018

Validating last SKR with HSM...
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-07-01T00:00:00 2010-07-15T23:59:59  55138,41248   19036
2  2010-07-11T00:00:00 2010-07-25T23:59:59  41248         19036
3  2010-07-21T00:00:00 2010-08-04T23:59:59  41248         19036
4  2010-07-31T00:00:00 2010-08-14T23:59:59  41248         19036
5  2010-08-10T00:00:00 2010-08-24T23:59:59  41248         19036
6  2010-08-20T00:00:00 2010-09-03T23:59:59  41248         19036
7  2010-08-30T00:00:00 2010-09-13T23:59:59  41248         19036
8  2010-09-09T00:00:00 2010-09-24T00:00:00  41248         19036
9  2010-09-20T00:00:00 2010-10-05T23:59:59  40288,41248   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2010-q4-1.xml...
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  40288,41248
2  2010-10-11T00:00:00 2010-10-25T23:59:59  40288
3  2010-10-21T00:00:00 2010-11-04T23:59:59  40288
4  2010-10-31T00:00:00 2010-11-14T23:59:59  40288
5  2010-11-10T00:00:00 2010-11-24T23:59:59  40288
6  2010-11-20T00:00:00 2010-12-04T23:59:59  40288
7  2010-11-30T00:00:00 2010-12-14T23:59:59  40288
8  2010-12-10T00:00:00 2010-12-25T00:00:00  40288
9  2010-12-21T00:00:00 2011-01-05T23:59:59  21639,40288
...PASSED.

SHA256 hash of KSR:
A17E539793B2611112C4F591A06AF4FBC2221DDDD71794BC72D5AEE910C72543
>> ratchet insurgent dwelling mosquito playhouse pioneer fallout Babylon atlas reproduce vapor miracle
ragtime hamburger upshot Wichita snapshot candidate Belfast tambourine stopwatch bookseller Pluto
pyramid highchair specialist robust ultimate assume retraction bombast decimal <<
Is this correct (y/N)? y

Generated new SKR in /media/KSR/skr-root-2010-q4-1.xml
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  40288,41248   19036
2  2010-10-11T00:00:00 2010-10-25T23:59:59  40288         19036
3  2010-10-21T00:00:00 2010-11-04T23:59:59  40288         19036
4  2010-10-31T00:00:00 2010-11-14T23:59:59  40288         19036
5  2010-11-10T00:00:00 2010-11-24T23:59:59  40288         19036
6  2010-11-20T00:00:00 2010-12-04T23:59:59  40288         19036
7  2010-11-30T00:00:00 2010-12-14T23:59:59  40288         19036
8  2010-12-10T00:00:00 2010-12-25T00:00:00  40288         19036
9  2010-12-21T00:00:00 2011-01-05T23:59:59  40288,21639   19036

SHA256 hash of SKR:
00CC341B7B3BAEE2E62B1AA6A58DEF07F02E4950E959E6A6ACBD7CEFF2741257
>> aardvark revolver choking bravado kickoff councilman robust tomorrow tracker Cherokee beehive
paragon reindeer microscope uncut amusement unearth coherence deckhand embezzle treadmill examine
tracker paragon ribcage quantity kiwi unravel uproot hydraulic atlas Eskimo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20100712-224426.log **********
```

Figure 1

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
41.	CA prints out a sufficient number of copies for participants using `for i in $(seq X); do printlog ksrsigner-20170202-*.log; done` where ksrsigner-**20170202**-*.log is replaced by log output file displayed by program. This generates **X** copies and hands copies to participants.		
42.	IW1 attaches a copy to his/her script.		

Backup Newly Created SKR

Step	Activity	Initials	Time
43.	CA copies the contents of the KSR FD by executing `cp –p /media/KSR/* .` for posting back to RZM. Confirm overwrite by typing "**y**", then press enter		

44.	CA lists the contents of KSR FD by executing
	`ls –ltr /media/KSR`
	flushes the system buffers by executing
	`sync`
	then unmounts the KSR FD by executing
	`umount /media/KSR`		

45.	CA removes the FD **KSR** containing SKR and gives it to the RZM representative.		

Disable/Deactivate HSM3

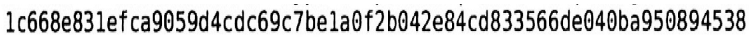
Step	Activity	Initials	Time
46.	CA ensures to utilize the cards that were NOT used on the prior steps. CA performs the following steps to deactivate the HSM: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"2.Set Offline"** press **ENT** to confirm c) When **"Set Offline?"** is displayed, press **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** press **ENT** f) When **"Remove Card?"** is displayed, remove 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		

Ceremony Break

Step	Activity	Initials	Time
47.	CA initiates the ceremony break and requests the TCRs to leave the TEBs with SO cards on the ceremony table visible to the audit cameras. **Note: All equipment and TEBs on the ceremony table should be visible to the audit cameras.**		
48.	CA divides the participants leaving the ceremony room in groups and ensures the following is enforced: • (1) CA and (1) IW are at the ceremony table • At least (2) Crypto Officers and (1) Auditor are present in the ceremony room during ceremony break • Audit Cameras are never obstructed CA, IW or SA escorts each group of participants out of the ceremony room for ceremony break.		
49.	Once all groups have returned to the ceremony room, CA ensures that all participants are present, then individually distributes the TEBs containing the SO cards to the TCRs.		

Act 3. KSK-2017 Import

Verify Transported Materials

Step	Activity	Initials	Time
1.	CA inspects the APP Key TEBs for tamper evidence; reads out the TEB # while IW1 observes and matches it with the ceremony 27 and media deposit annotated scripts. CA then places the items on the cardholder. **APP Key (KSK-2017): TEB# BB46584642** **APP Key (KSK-2017): TEB# BB46584643**		
2.	CA plugs the **ceremony 27** HSMFD into the free USB slot on the laptop and waits for the OS to recognize it (as HSMFD_). CA displays the HSMFD contents to all participants then closes the file system window.		
3.	CA calculates the sha256 hash of the **ceremony 27** HSMFD by executing `find -P /media/HSMFD_ -type f -print0 | sort -z | xargs -0 cat | sha256sum` IW1 confirms the result matches the sha256 hash of the HSMFD from the **Ceremony 27** annotated script. (image from Ceremony 27 annotated script).  1c668e831efca9059d4cdc69c7be1a0f2b042e84cd833566de040ba950894538 **Note: The CA should assign some participants to confirm the hash displayed on the TV screen while the others confirm the hash written on this ceremony script.**		

Update Keymap File

Step	Activity	Initials	Time

4.	CA updates the keymap file of the HSMFD using the **ceremony 27 HSMFD** by executing
	`cp -p /media/HSMFD_/KSKSlotDB.db .`
	When "**`cp: overwrite `./KSKSlotDB.db'?`**" is displayed, types "**y**", then press enter.
	CA confirms both files are identical by executing
	`diff /media/HSMFD_/KSKSlotDB.db KSKSlotDB.db`		

5.	CA flushes the system buffers and unmounts the **ceremony 27 HSMFD** by executing
	`sync`
	then
	`umount /media/HSMFD_`		

6.	CA removes the **ceremony 27 HSMFD** from the laptop; takes the backup **ceremony 27 HSMFD** from the cardholder, then gives both to the RKOS.		

Create Temporary CO Cards

Step	Activity	Initials	Time
7.	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 SO cards to the CA to be placed on the cardholder visible to everyone. **CO 1: Arbogast Fabian** **SO TEB # BB46584663** **CO 2: Dmitry Burkov** **SO TEB # BB46584652** **CO 3: Joao Damas** **SO TEB # BB21820433** **CO 4: Carlos Martinez** **SO TEB # BB46584665** **CO 6: Nicolas Antoniello** **SO TEB # BB46584667** **CO 7: Subramanian Moonesamy** **SO TEB # BB46584668** **Note: There are (2) sets of SO cards that cannot be mixed. Cards in different sets do not work together.**		

Step	Activity	Initials	Time
8.	CA ensures to utilize **3 SO** cards from the same set to create temporary **Crypto Officer (CO)** cards: a) Utilize the HSM's keyboard and scroll through menu using **<>** key b) Select **"7.Role Mgmt"** press **ENT** to confirm c) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder d) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** e) When **"Remove Card?"** is displayed, remove card f) Repeat steps c) to e) for the 2nd and 3rd SO cards 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"** and press **ENT** to confirm k) When **"Num Req Cards?"** is displayed, enter **"2"** and press **ENT** to confirm l) When **"Insert Card #?"** is displayed, insert the proper sequence of **CO** card from the cardholder m) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** n) When **"Remove Card?"** is displayed, remove 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 twice** to return to the main menu **"Secured"** IW1 records the used SO cards below. CA returns all cards on the cardholder after use. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

Import KSK-2017 to HSM3

Step	Activity	Initials	Time
9.	CA performs the following steps to import the KSK-2017 using **2 CO Cards** a) Utilize the HSM's keyboard and scroll through menu using **<>** key b) Select **"5.Key Mgmt"** press **ENT** to confirm c) When **"Insert Card CO #?"** is displayed, insert the CO card from the cardholder d) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** e) When **"Remove Card?"** is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select **"3.App Keys"** press **ENT** to confirm h) Select **"2.Restore"** press **ENT** to confirm i) When **"Restore?"** is displayed, press **ENT** to confirm j) When **"Which Media?"** is displayed, select **"2. From Card"** and press **ENT** to confirm k) When **"Insert Card #?"** is displayed, insert one of the **KSK-2017 APP Key card** from the cardholder l) When **"Remove Card?"** is displayed, remove card m) When **"Restore Complete"** is displayed, press **ENT** to confirm n) Press **CLR twice** to return to the main menu **"Secured"** CA returns all cards on the cardholder after use.		

Enable/Activate HSM3

Step	Activity	Initials	Time
10.	CA performs the following steps to activate the **HSM** using **3 OP Cards** a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"1.Set Online"** press **ENT** to confirm c) When **"Set Online?"** is displayed, press **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card 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 HSM

Step	Activity	Initials	Time
11.	CA switches to the terminal window and tests network connectivity between laptop and HSM by executing `ping 192.168.0.2` Confirm responses, then press Ctrl-C to terminate ping.		

Verify Imported APP Key KSK-2017

Step	Activity	Initials	Time
12.	CA verifies that the KSK-2017 was successfully imported by executing `keybackup –l –P 123456` IW confirms that the KSK-2017 keypair label **Klajeyz** is displayed.		

Generate and Verify Certificate Signing Request

Step	Activity	Initials	Time
13.	CA generates a Certificate Signing Request (CSR) by executing `kskgen Klajeyz` When **"Activate HSM prior to accepting in the affirmative! (y/n)"** is displayed, confirm that the HSM's **"READY"** LED is on. Type **"y"**, then press enter to confirm If **"slot"** is asked type **0**, then press enter		
14.	CA checks the integrity of the CSR by executing `displaycsr Klajeyz.csr` a) IW verifies the **DS resource record** matches with the printed copy of the **ceremony 27 annotated script**. Output should look like sample Figure 2 b) Press SPACE bar until the end of display, then type "q" to end.		

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: O=Public Technical Identifiers, OU=Cryptographic Business Operations, CN=Root Zone
KSK 2016-10-27T18:50:19+00:00/1.3.6.1.4.1.1000.53=. IN DS 20326 8 2
E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ac:ff:b4:09:bc:c9:39:f8:31:f7:a1:e5:ec:88:
                    f7:a5:92:55:ec:53:04:0b:e4:32:02:73:90:a4:ce:
                    89:6d:6f:90:86:f3:c5:e1:77:fb:fe:11:81:63:aa:
                    ec:7a:f1:46:2c:47:94:59:44:c4:e2:c0:26:be:5e:
                    98:bb:cd:ed:25:97:82:72:e1:e3:e0:79:c5:09:4d:
                    57:3f:0e:83:c9:2f:02:b3:2d:35:13:b1:55:0b:82:
                    69:29:c8:0d:d0:f9:2c:ac:96:6d:17:76:9f:d5:86:
                    7b:64:7c:3f:38:02:9a:bd:c4:81:52:eb:8f:20:71:
                    59:ec:c5:d2:32:c7:c1:53:7c:79:f4:b7:ac:28:ff:
                    11:68:2f:21:68:1b:f6:d6:ab:a5:55:03:2b:f6:f9:
                    f0:36:be:b2:aa:a5:b3:77:8d:6e:eb:fb:a6:bf:9e:
                    a1:91:be:4a:b0:ca:ea:75:9e:2f:77:3a:1f:90:29:
                    c7:3e:cb:8d:57:35:b9:32:1d:b0:85:f1:b8:e2:d8:
                    03:8f:e2:94:19:92:54:8c:ee:0d:67:dd:45:47:e1:
                    1d:d6:3a:f9:c9:fc:1c:54:66:fb:68:4c:f0:09:d7:
                    19:7c:2c:f7:9e:79:2a:b5:01:e6:a8:a1:ca:51:9a:
                    f2:cb:9b:5f:63:67:e9:4c:0d:47:50:24:51:35:7b:
                    e1:b5
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
        80:8a:21:20:14:8a:5f:d8:91:e4:81:ac:e8:07:dd:e9:47:32:
        ed:ba:2e:a5:06:47:7e:a5:66:a9:2f:aa:b3:1a:df:f6:44:b1:
        44:8f:2c:4f:76:63:06:10:e7:52:d7:40:f2:2d:c8:b3:d5:7a:
        ad:4f:74:38:c8:39:68:54:e7:21:ba:c1:5a:af:29:39:8d:11:
        66:5a:54:f3:f0:15:d2:db:6a:e5:3e:cc:e3:c2:d6:c5:60:2b:
        6a:1a:04:73:d6:0e:a5:10:cc:26:9e:bc:27:12:a2:14:84:95:
        6c:03:cb:60:8d:ac:d9:74:41:b4:c5:20:1f:9d:f0:37:5c:8b:
        5c:9f:17:4c:e0:3a:79:db:c1:58:75:6d:b0:af:60:85:8f:fe:
        bf:f6:93:21:49:cc:55:e2:49:fc:8d:15:89:d4:2d:48:1d:d2:
        ee:52:11:7e:d2:74:89:ba:34:fd:54:c3:f7:d2:90:bc:9e:a9:
        95:cb:6a:41:9d:2a:eb:54:0d:3b:65:57:9f:ce:19:29:64:7f:
        1c:a6:fb:49:f9:15:2f:af:0a:dc:88:03:be:34:cd:fd:db:67:
        76:dc:59:61:98:25:30:94:f9:72:f4:ce:4c:61:3c:b7:d4:30:
        26:b1:78:fa:20:ab:83:04:e1:dd:31:58:24:e7:98:8a:d3:01:
        1b:bb:80:d7
```

Figure 2

Disable/Deactivate HSM3 and Place into the TEB

Step	Activity	Initials	Time
15.	CA pushes the "RESTART" button on the HSM to deactivate it. CA confirms that the HSM displays "**Secured**" and **"READY"** led is **OFF.**		
16.	CA switches the HSM power OFF and disconnects it from power and laptop (serial and Ethernet) connections. **Note: DO NOT unplug the connections on the laptop end**		
17.	CA places the HSM into a prepared TEB and seals it.		
18.	CA reads out TEB # and HSM serial #, shows item to participants, then IW1 confirms TEB # and HSM serial # below. **HSM3: TEB# BB51184611 / serial # H1403033** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. CA then places the HSM TEB on the equipment cart.		

Power Up HSM4

Step	Activity	Initials	Time
1.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and HSM serial # while IW1 observes and matches it with the prior ceremony script in this facility. **HSM4: TEB# BB24646625 / serial# H1411006**		
2.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable and Ethernet cable in **LAN** port.		
3.	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. **HSM4: serial# H1411006** **Note: The date/time on the HSM is not used as a reference for logging and timestamp.**		

Import KSK-2017 to HSM4

Step	Activity	Initials	Time
19.	CA performs the following steps to import the KSK-2017 using **2 CO Cards** a) Utilize the HSM's keyboard and scroll through menu using **<>** key b) Select **"5.Key Mgmt"** press **ENT** to confirm c) When **"Insert Card CO #?"** is displayed, insert the CO card from the cardholder d) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** e) When **"Remove Card?"** is displayed, remove card f) Repeat steps c) to e) for the 2nd CO card g) Select **"3.App Keys"** press **ENT** to confirm h) Select **"2.Restore"** press **ENT** to confirm i) When **"Restore?"** is displayed, press **ENT** to confirm j) When **"Which Media?"** is displayed, select **"2. From Card"** and press **ENT** to confirm k) When **"Insert Card #?"** is displayed, insert the other **KSK-2017 APP Key card** from the cardholder l) When **"Remove Card?"** is displayed, remove card m) When **"Restore Complete"** is displayed, press **ENT** to confirm n) Press **CLR twice** to return to the main menu **"Secured"** CA returns all cards on the cardholder after use.		

Enable/Activate HSM4

Step	Activity	Initials	Time
20.	CA performs the following steps to activate the **HSM** using **3 OP Cards** a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"1.Set Online"** press **ENT** to confirm c) When **"Set Online?"** is displayed, press **ENT** to confirm d) When **"Insert Card OP #?"** is displayed, insert the OP card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and press **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd OP card 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 HSM

Step	Activity	Initials	Time
21.	CA switches to the terminal window and tests network connectivity between laptop and HSM by executing `ping 192.168.0.2` Confirm responses, then press "Ctrl C" to terminate ping.		

Verify Imported Key KSK-2017

Step	Activity	Initials	Time
22.	CA verifies that the KSK-2017 is successfully imported by executing `keybackup -l -P 123456` IW confirms that the KSK-2017 keypair label **Klajeyz** is displayed.		

Generate and Verify CSR

Step	Activity	Initials	Time

23.	CA generates a CSR on a temporary folder by executing
	`cd /tmp`
	then
	`kskgen Klajeyz`
	When **"Activate HSM prior to accepting in the affirmative! (y/n)"** is displayed, confirm that the HSM's **"READY"** LED is on.
	Type **"y"**, then press enter to confirm
	If **"slot"** is asked type **0.**		

24.	CA checks the integrity of the CSR by executing
	`displaycsr Klajeyz.csr`
	a) IW verifies the DS resource record matches with the printed copy of the **ceremony 27 annotated script**. Output should look like sample Figure 2
	b) Press "SPACE bar" until the end of display, then type "q" to end.
	c) CA returns to the HSMFD folder by executing
	`cd /media/HSMFD`		

Act 5. Secure Hardware and Close Ceremony

Disable/Deactivate HSM4 and Place into the TEB

Step	Activity	Initials	Time
1.	CA switches to the ttyaudit terminal window and pushes the “RESTART” button on the HSM to deactivate it. CA confirms that the HSM displays “**Secured**” and **“READY”** led is **OFF.**		

Clear and Destroy Temporary CO Cards

Step	Activity	Initials	Time
2.	CA ensures to utilize the **same set** of **3 SO cards** to clear the **CO** cards: a) Utilize the HSM’s keyboard and scroll through menu using **<>** key b) Select **“7.Role Mgmt”** press **ENT** to confirm c) When **“Insert Card SO #?”** is displayed, insert the SO card from the cardholder d) When **“PIN?”** is displayed, enter **“11223344”** and press **ENT** e) When **“Remove Card?”** is displayed, remove 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”** and press **ENT** to confirm j) When **“Insert Card #?”** is displayed, CA takes the temporary **CO** card form the cardholder, shows it to the audit camera above, then inserts it into the HSM’s card reader k) When **“PIN?”** is displayed, enter **“11223344”** and press **ENT** l) When **“Remove Card?”** is displayed, remove card m) Repeat steps j) to l) for the 2nd **CO card**, then proceed to step n) n) Press **CLR** to return to the main menu **“Secured”** IW1 records the used cards below. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7 CA uses the shredder to destroy the cleared CO cards.		

Place HSM4 into the TEB

Step	Activity	Initials	Time
3.	CA switches the HSM power OFF and disconnects it from power and laptop (serial and Ethernet) connections. **Note: DO NOT unplug the connections on the laptop end**		
4.	CA places the HSM into a prepared TEB and seals it.		
5.	CA reads out TEB # and HSM serial #, shows item to participants, then IW1 confirms TEB # and HSM serial # below. **HSM4: TEB# BB51184612 / serial # H1411006** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. CA then places the HSM TEB on the equipment cart.		

Stop Logging of Serial Port Activity and Terminal Output

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

Backup HSMFD

Step	Activity	Initials	Time
8.	CA sets dotglob by executing `shopt –s dotglob` This allows copying everything in the original HSMFD.		
9.	CA calculates the sha256hash of the contents on the original HSMFD. `find -P /media/HSMFD -type f –print0 | sort -z | xargs -0 cat | sha256sum`		
10.	CA copies and pastes the command and the sha256 hash on a Text Editor **Applications > Accessories > Text Editor**		
11.	CA prints three copies of the hash, then writes "**KSK 28**" on all the pages One for the audit bundle and the other for the HSMFD packages.		
12.	CA displays the contents of HSMFD by executing `ls –ltr`		
13.	CA plugs a blank FD labeled HSMFD into the free USB slot on the laptop and waits for the OS to recognize it (as HSMFD_). CA closes the file system window and creates a backup of the HSMFD by executing `cp -Rp * /media/HSMFD_`		
14.	CA displays the contents of HSMFD_ by executing `ls –ltr /media/HSMFD_`		
15.	CA calculates the sha256 hash of the HSMFD copy by executing `find -P /media/HSMFD_ -type f –print0 | sort -z | xargs -0 cat | sha256sum` Confirm that the result matches the original HSMFD sha256 hash result by using the text editor to copy and paste for comparison.		
16.	CA unmounts the HSMFD copy by executing `umount /media/HSMFD_`		
17.	CA removes **HSMFD_** and places it on the holder.		
18.	CA repeats step 13 to 17 for the 2nd copy.		
19.	CA repeats step 13 to 17 for the 3rd copy.		
20.	CA repeats step 13 to 17 for the 4th copy.		
21.	CA repeats step 13 to 17 for the 5th copy.		
22.	CA repeats step 13 to 17 for the 6th copy.		

Print Serial Port Activity and Terminal Output Logs

Step	Activity	Initials	Time

23.	CA prints out a hard copy of logging information by executing
	`enscript -2Gr -# 1 script-20170202.log`
	`enscript –Gr -# 1 --font=”Courier8” ttyaudit-ttyUSB*-20170202-*.log`
	IW1 attaches the printed copies to his/her annotated script.
	Note: Ignore the error regarding non-printable characters if prompted.		

Place HSMFD and OS DVD into the TEB

Step	Activity	Initials	Time

24.	CA unmounts the HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
	CA removes the HSMFD and places it on the holder		

25.	CA performs the following to turn off the laptop. a) CA turns off the laptop by pressing the power switch b) CA turns on the laptop by pressing the power switch and immediately removes the OS DVD from the laptop DVD drive c) CA turns off the laptop again by pressing the power switch		
26.	CA places **(2)** HSMFDs, **(2)** OS/DVD and **(1)** paper with printed HSMFD hash into the prepared TEB, then seals it. CA reads out the TEB # and shows it to IW1 and participants to confirm. **OS DVD (release 20161014) + HSMFD: TEB# BB46584447**		
27.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. CA then places the OS/DVD and HSMFD TEB on the equipment cart.		

Place APP Key Backup Cards into the TEB

Step	Activity	Initials	Time
28.	CA performs the following to secure the APP Key backups for this KSK facility. a) CA places **(2)** APP Key cards into the plastic case. b) CA places the plastic case, **(1)** HSMFD and **(1)** printed copy of the HSMFD HASH into the prepared TEB, then seals it. c) CA and IW initials the TEB using a ballpoint pen and keeps the sealing strip for later inventory. d) CA reads out the TEB # and shows it to all participants to compare with the TEB # below. e) CA then places the APP Key TEB on the equipment cart. **APP Key: TEB # BB46584449**		

Distribute HSMFDs

Step	Activity	Initials	Time
29.	CA distributes the remaining HSMFDs to IW1 (2 for audit bundles) and to RKOS (2 for posting the SKR to RZM and for review and process improvements)		

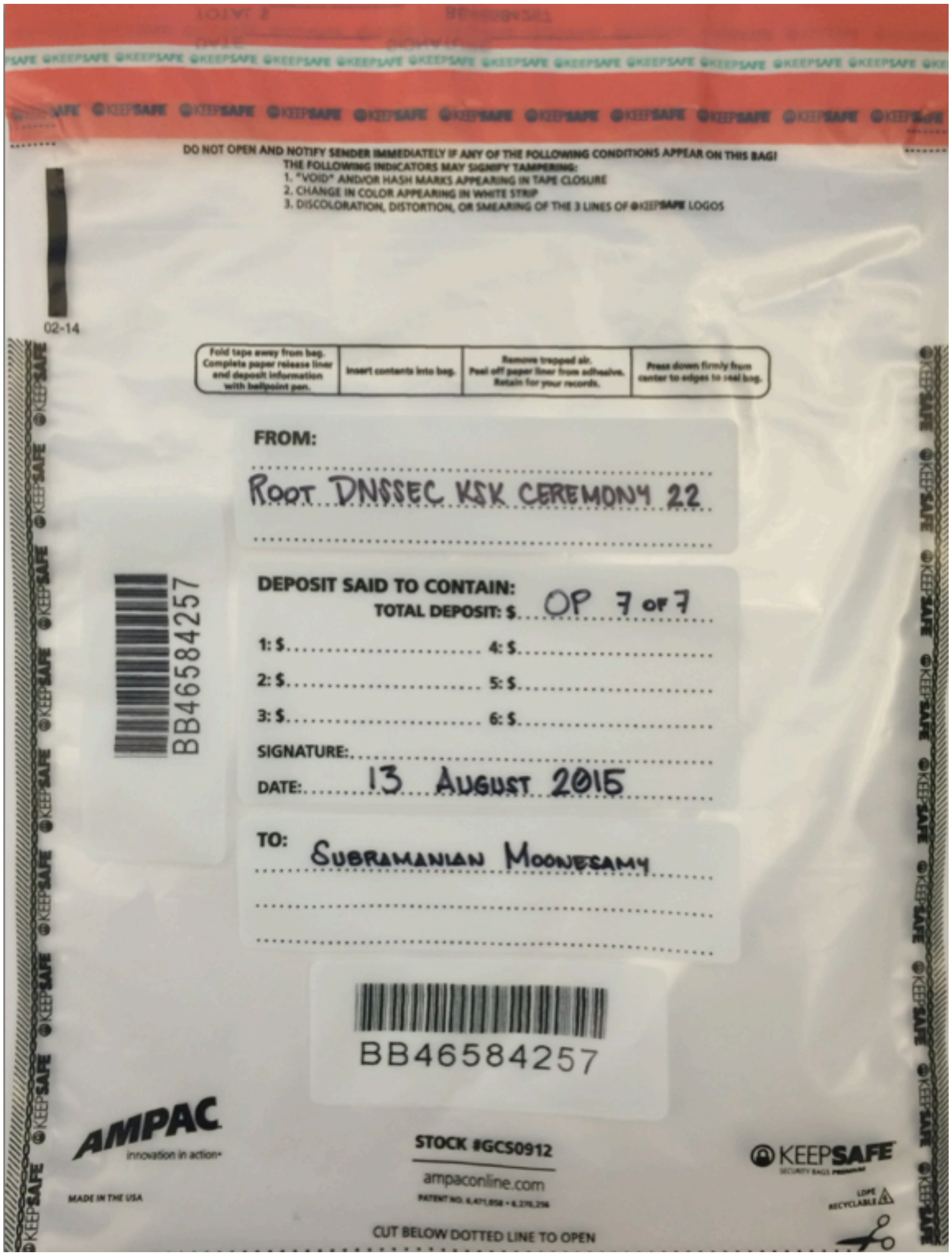
Place Laptop into the TEB

Step	Activity	Initials	Time
30.	CA disconnects all connections to the laptop including printer, display, network and power; places it into a prepared TEB, then seals it. CA reads out the TEB # and shows it to IW1 and participants to confirm. **Laptop1: TEB# BB51184609 / serial # 37240147333**		
31.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA places the Laptop TEB on the equipment cart.		

Place OP and SO Cards into the TEB

Step	Activity	Initials	Time
32.	One by one, CA calls each COs to the ceremony table to place the OP and SO cards into the TEB by following the steps shown below. a) CA takes the (2) TEBs prepared for the CO, then reads out each TEB # and description while showing it. b) CO takes his/her OP card from the cardholder; places it into the plastic case, then gives it to the CA c) CO places his/her SO cards from the cardholder; places them into the plastic case, then gives it to the CA d) CA places each plastic case into the prepared TEBs, seals it and initials it using a ballpoint pen, then IW1 keeps sealing strips for later inventory. e) IW1 inspects each TEBs, confirms it with the description on the table next page, then initials the TEB using a ballpoint pen. f) CA hands each TEBs containing the OP and the SO cards to the CO. g) CO inspects and verifies TEB # and contents, then initials his/her TEB using a ballpoint pen. h) CO writes the completion time and signature on the table on IW1's script, then IW1 initials the entry. i) CO returns to his/her seat with the TEBs, being careful not to poke or puncture TEBs. **CO 1: Arbogast Fabian** **OP TEB # BB46584450** **SO TEB # BB46584451** **CO 2: Dmitry Burkov** **OP TEB # BB46584452** **SO TEB # BB46584453** **CO 3: Joao Damas** **OP TEB # BB46584454** **SO TEB # BB46584455** **CO 4: Carlos Martinez** **OP TEB # BB46584456** **SO TEB # BB46584457** **CO 6: Nicolas Antoniello** **OP TEB # BB46584458** **SO TEB # BB46584459** **CO 7: Subramanian Moonesamy** **OP TEB # BB46584460** **SO TEB # BB46584461**		

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584450	Arbogast Fabian		___ February 2017		
CO 1	SO 1 of 7	BB46584451	Arbogast Fabian		___ February 2017		
CO 2	OP 2 of 7	BB46584452	Dmitry Burkov		___ February 2017		
CO 2	SO 2 of 7	BB46584453	Dmitry Burkov		___ February 2017		
CO 3	OP 3 of 7	BB46584454	Joao Damas		___ February 2017		
CO 3	SO 3 of 7	BB46584455	Joao Damas		___ February 2017		
CO 4	OP 4 of 7	BB46584456	Carlos Martinez		___ February 2017		
CO 4	SO 4 of 7	BB46584457	Carlos Martinez		___ February 2017		
CO 6	OP 6 of 7	BB46584458	Nicolas Antoniello		___ February 2017		
CO 6	SO 6 of 7	BB46584459	Nicolas Antoniello		___ February 2017		
CO 7	OP 7 of 7	BB46584460	Subramanian Moonesamy		___ February 2017		
CO 7	SO 7 of 7	BB46584461	Subramanian Moonesamy		___ February 2017		



DO NOT OPEN AND NOTIFY SENDER IMMEDIATELY IF ANY OF THE FOLLOWING CONDITIONS APPEAR ON THIS BAG!
THE FOLLOWING INDICATORS MAY SIGNIFY TAMPERING:
1. "VOID" AND/OR HASH MARKS APPEARING IN TAPE CLOSURE
2. CHANGE IN COLOR APPEARING IN WHITE STRIP
3. DISCOLORATION, DISTORTION, OR SMEARING OF THE 3 LINES OF KEEPSAFE LOGOS

02-14

Fold tape away from bag. Complete paper release liner and deposit information with ballpoint pen.	Insert contents into bag.	Remove trapped air. Peel off paper liner from adhesive. Retain for your records.	Press down firmly from center to edges to seal bag.

FROM:
ROOT DNSSEC KSK CEREMONY 22

DEPOSIT SAID TO CONTAIN:
TOTAL DEPOSIT: $ OP 7 OF 7
1: $ 4: $
2: $ 5: $
3: $ 6: $
SIGNATURE:
DATE: 13 AUGUST 2015

BB46584257

TO: SUBRAMANIAN MOONESAMY

BB46584257

AMPAC
innovation in action
MADE IN THE USA

STOCK #GCS0912
ampaconline.com
PATENT NO. 6,471,058 • 6,270,256

KEEPSAFE
SECURITY BAGS PREMIUM
LDPE RECYCLABLE

CUT BELOW DOTTED LINE TO OPEN

Figure 3

Returning Equipment to Safe #1

Step	Activity	Initials	Time
33.	CA, IW1, SSC1 opens the safe room and enter with the equipment cart.		
34.	SSC1 opens the Safe #1 shielding combination from camera.		
35.	SSC1 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 then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
36.	CA **CAREFULLY** removes each of the HSM TEBs from the equipment cart; reads out the TEB # and HSM serial #, then **CAREFULLY** places it into the 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# BB51184611 / serial # H1403033** **HSM4: TEB# BB51184612 / serial # H1411006**		
37.	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: TEB# BB51184609 / serial # 37240147333** **OS DVD (release 20161014) + HSMFD: TEB# BB46584447** **APP Key: TEB# BB46584449**		

Close Equipment Safe #1

Step	Activity	Initials	Time
38.	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.		
39.	SSC1 returns the 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.		
40.	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
41.	CA and IW1 brings a flashlight then escorts SSC2, COs with their OP Card and SO Card TEBs into the safe room.		
42.	SSC2, while shielding combination from camera, opens Safe #2.		
43.	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 then initials it.		

CO Returns Credentials to Safe #2

Step	Activity	Initials	Time
44.	One by one, the selected CO returns the OP cards and SO cards (in TEB) by following the steps shown below. a) CO reads out their OP card TEB # and SO card TEB # and verifies its integrity b) 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** c) CO places all his/her TEBs; verifies the integrity of the safe deposit box and reads out the box number then locks it. d) CO writes the date/time and signature on the safe log where the return of his/her OP and SO cards are indicated. e) IW1 verifies the completed safe log entries then initials it. Repeat these steps until all required cards listed below are returned. **CO 1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46584450** **SO TEB # BB46584451** **CO 2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46584452** **SO TEB # BB46584453** **CO 3: Joao Damas** **Box # 1071** **OP TEB # BB46584454** **SO TEB # BB46584455** **CO 4: Carlos Martinez** **Box # 1068** **OP TEB # BB46584456** **SO TEB # BB46584457** **CO 6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584458** **SO TEB # BB46584459** **CO 7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46584460** **SO TEB # BB46584461**		

Close Credential Safe #2

Step	Activity	Initials	Time
45.	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.		
46.	SSC2 returns the log back in the Safe 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.		
47.	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
48.	One by one, the CA calls all participants to the ceremony table to confirm the printed name and date and to **signs IW1’s coversheet declaring that this script is a true and an accurate record of the ceremony.** IW1 records the completion time once all participants have signed the coversheet.		
49.	CA reviews IW1’s script and signs the coversheet.		

Stop Online Streaming

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

Sign Out of Ceremony Room

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

Stop Video Recording

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

Bundle Audit Materials

Step	Activity	Initials	Time
53.	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 and Intrusion Detection System (Range is **10/27/2016 – 02/03/2017**) e) The IW1 attestation (A.1 below) f) SA attestation (A.2, A.3 below) All in a TEB labeled **"Root DNSSEC KSK Ceremony 28"**, dated and signed by **IW1 and CA**. Off-site audit bundle is delivered to off-site storage. **The CA holds the ultimate responsibility for finalizing the audit bundle.**		

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 placed within a tamper-evident bag, 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 for the original audit bundle and the other for duplicate.

4. Logs from the Physical Access Control (PAC) and Intrusion Detection System (IDS) (SA1)
One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC and IDS configuration review, the list of enrolled users, the event log file and the configuration audit log file in each audit bundle. Each placed in a tamper-evident bag, 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 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. Make sure 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.

Yuko Green

____

Date: ___ February 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 **11 August 2016 00:00 UTC** to now.

Connor Barthold

____

Date: ___ February 2017

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: ___ February 2017