Internet Corporation for Assigned Names and Numbers

Root DNSSEC KSK Ceremony 26

Thursday August 11, 2016

ICANN KSK Facility@Equinix LA3
1920 East Maple Avenue, El Segundo, CA 90245

This ceremony is executed under the
DNSSEC Practices Statement for the Root Zone KSK Operator Version 3rd Edition (2015-10-01)

Abbreviations

TEB =	Tamper Evident Bag (AMPAC, item #GCS1013, item #GCS0912 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large)	**SO =**	Security Officer	**CO =**	Crypto Officer
OP =	Operator	**CA =**	Ceremony Administrator	**IW =**	Internal Witness
SW =	Staff Witness	**SSC =**	Safe Security Controller	**EW =**	External Witness
MC =	Master of Ceremony	**IKOS =**	ICANN KSK Operations Security	**SA =**	System Administrator
AUD =	Third Party Auditor	**RZM =**	Root Zone Maintainer	**HSM =**	Hardware Security Module
FD =	Flash Drive	**KSR =**	Key Signing Request	**SKR =**	Signed Key Response

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		12 August 2016	
IW1	Owen Smigelski / ICANN			
SSC1	Anand Mishra / ICANN			
SSC2	Leo Vegoda / ICANN			
CO1	Arbogast Fabian / TZ			
CO2	Dmitry Burkov / RU			
CO4	Carlos Martinez / UY			
CO5	Olafur Gudmundsson / IS			
CO6	Nicolas Antoniello / UY			
CO7	Subramanian Moonesamy / MU			
RZM	Duane Wessels/ Verisign			
RZM	Sanju Varghese / Verisign			
RZM	Andrew Kim / Verisign			
AUD	Jacky Kwong / PricewaterhouseCoopers			
AUD	Laura Sacks / PricewaterhouseCoopers			
SA1	Connor Barthold / ICANN			
SA2	Brian Martin / ICANN			
CA2 / IKOS	Alberto Duero / ICANN			
IW2 / IKOS	Andres Pavez / ICANN			
CA3	Edward Lewis / ICANN			
SW	Matt Larson / ICANN			
SW	Shauna Royston / ICANN			

Note: 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.

Note: Dual Occupancy enforced. CA leads ceremony. Only CAs, IWs, or SAs can enter 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 in safe room. Participants must sign in and out of ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before 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 streaming is live.		
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 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.		
8.	SSC2, while shielding combination from camera, opens Safe #2.		
9.	SSC2 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC2. SSC2 appends the new safe log then prints name, date, time, signature, and reason (i.e. “open safe”) in safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		

COs Extract Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	One by one, the selected CO retrieves the required OP cards and SO cards following the steps shown below. a) With the assistance of CA (and his/her common key), opens her/his safe deposit box. **# Common Key is bottom lock and CO Key is top lock** b) Retains OP TEB and SO TEB then locks the safe deposit box. c) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below. d) Makes an entry in safe log indicating OP TEB and SO TEB removal with box #, printed name, date, time and signature. **(Note: If log entry is pre-printed, verify the entry, record time of completion and sign.)** Repeat these steps until all required cards are removed. IW1 initials this entry when all COs have finished. **CO 1: Arbogast Fabian** **Box #: 1791** **OP TEB # BB46584279 (Retain)** **SO TEB # BB46584262 (Retain)** **CO 2: Dmitry Burkov** **Box #: 1793** **OP TEB # BB46584280 (Retain)** **SO TEB # BB46584256 (Retain)** **CO 4: Carlos Martinez** **Box #: 1068** **OP TEB # BB46584253 (Retain)** **SO TEB # BB46584254 (Retain)** **CO 5: Olafur Gudmundsson** **Box #: 1789** **OP TEB # BB46584251 (Retain)** **SO TEB # BB46584252 (Retain)** **CO 6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584283 (Retain)** **SO TEB # BB46584284 (Retain)** **CO 7: Subramanian Moonesamy** **Box #: 1792** **OP TEB # BB46584285 (Retain)** **SO TEB # BB46584258 (Retain)**		

Close Credential Safe #2

Step	Activity	Initials	Time
11.	Once all relevant deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
12.	SSC2 puts log in safe and locks Safe #2 (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 cards and SO cards (if applicable) in TEBs, closing the door behind them.		

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	After a one (1) minute delay, 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 current page to the camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		

Remove Equipment from Safe #1

Step	Activity	Initials	Time
17.	**CA CAREFULLY removes HSM1, HSM2 and HSM4 (in TEB)** from the safe and completes the entry on the safe log indicating HSMs Removal, TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** **HSM1: TEB# BB24646605 / serial # K6002020** **HSM2: TEB# BB24646669 / serial # K6002018** **HSM4: TEB# BB24646664 / serial # H1411006** Verify the integrity of the other HSMs that will not be used and return them to the safe. **HSM3: TEB# BB24646618 / serial # H1403033**		
18.	CA takes out the items listed below from the safe and completes the entry on the safe log indicating each item, TEB#, serial number if available. Printed name, date, time and signature. CA places the items on the equipment cart. IW1 initials each entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** **Laptop1 (Dell ATG6400): TEB# BB24646619 / serial # 37240147333** **O/S DVD (Rev600) + HSMFD: TEB# BB46584278** Verify the integrity of the other Laptop that will not be used this time and return it to the safe. **Laptop2 (Dell ATG6400): TEB# BB24646591 / serial# 7292928457**		

Close Equipment Safe #1 and exit safe room

Step	Activity	Initials	Time
19.	SSC1 makes an entry including printed name, date, time and signature on the safe log indicating, “Close safe”. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
20.	SSC1 puts log back in safe and locks Safe #1 (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 leave the safe room with the equipment cart, closing the door to the safe room securely 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 TEB # and serial # while IW1 observes and matches it to the prior entry in most recent key ceremony or acceptance script for this site. IW1 confirms the TEB # and serial # below. **Laptop1 (Dell ATG6400): TEB# BB24646619 / serial # 37240147333**		
2.	CA inspects the O/S DVD + HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior entry in most recent key ceremony script for this site. IW1 confirms the TEB # below. **O/S DVD (Rev600) + HSMFD: TEB# BB46584278**		
3.	CA takes the laptop, HSMFD and O/S DVD out of TEB placing it on the key ceremony table; discards TEBs; connects laptop power, external display, printer, general purpose external DVD drive and boots laptop from **O/S DVD (Rev600).**		
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 O/S DVD **release 20160503** into the external DVD drive, waits for it to be recognized by the O/S 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 SHA256 hash by executing
	`sha256sum /dev/scd1`
	`SHA256 hash for release 20160503:`
	6cabb3c146aa13fbc9a9d61488b2c6f8c7e9e723a89b8574b0288578a65cc0f5
	IW1 and participants confirm that the result matches the above, which also matches the one published on:
	https://data.iana.org/ksk-ceremony/25/KC-20160503.iso.sha256		

7.	CA removes the O/S 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 O/S DVD **release 20160503**.		
9.	IW1 records the date, time then affixes his/her signature upon successful completion of the O/S DVD release 20160503 acceptance testing: **O/S DVD Acceptance Test release 20160503** **Printed Name** **Owen Smigelski** **Date** **2016/08/11** **Time** _____ **Signature** _____		
10.	CA disconnects the general purpose external DVD drive from the laptop, then removes the O/S DVD by performing: a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch and immediately remove the old O/S DVD **(Rev600)** from the laptop DVD drive c) Disconnect the laptop power to power off the laptop		
11.	CA discards all the old O/S DVD (Rev600) copies.		

Set Up Laptop

Step	Activity	Initials	Time
12.	CA connects the laptop power and boots the laptop using the new **O/S DVD release 20160503**.		
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 windows, CA executes: **`cp /usr/share/zoneinfo/UTC /etc/localtime`** When **"`cp: overwrite `/etc/localtime'?`"** is displayed, type **"`y`"** and press enter. then **`date -s "20160811 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 O/S, 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 unmounts 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 24** into the free USB slot on the laptop and waits for O/S to recognize the FD. CA lets participants view file names in the HSMFD then closes the file system window.		
23.	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 that is on the annotated script from the **Ceremony 24**. Previous hash should read as below (image from Ceremony 24 annotated script). `71eda78ef35290b984f3a6669cd9ba1ef0f76869279b612dea366b99a9675279` **Note: The CA should assign some attendees to confirm the hash displayed on the TV screen and the rest will confirm 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-20160811.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 HSM4

Step	Activity	Initials	Time
28.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM4: TEB# BB24646664 / serial # H1411006**		
29.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		
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 displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) **HSM4: serial # H1411006** **Note: The HSM date and time was set from the factory and will not be used as a reference**		

Enable/Activate HSM

Step	Activity	Initials	Time
31.	One by one, CA calls each COs listed below to inspect the TEB for tamper evidence, opens the TEB and hands the OP cards to the CA who places the cards in cardholder visible to all. **CO 1: Arbogast Fabian** **OP TEB # BB46584279** **CO 2: Dmitry Burkov** **OP TEB # BB46584280** **CO 4: Carlos Martinez** **OP TEB # BB46584253** **CO 5: Olafur Gudmundsson** **OP TEB # BB46584251** **CO 6: Nicolas Antoniello** **OP TEB # BB46584283** **CO 7: Subramanian Moonesamy** **OP TEB # BB46584285**		
32.	CA will perform the following steps to activate the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"1.Set Online"** hit **ENT** to confirm c) When **"Set Online?"** is displayed, 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"** and hit **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
33.	CA connects HSM to laptop using Ethernet cable in **LAN** port.		
34.	CA switches to the terminal window and tests network connectivity between laptop and HSM by entering **`ping 192.168.0.2`** and looking for responses. Ctrl-C to exit program.		

Insert 1st KSR to be signed

Step	Activity	Initials	Time
35.	The KSRs are downloaded to the KSRFD and transferred to the facility by the IKOS. CA plugs FD labeled **"KSR2048"** with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA shows the KSR file contents by: a) Double click file b) Select **DISPLAY** on the pop-up menu c) Maximize the window to show the contents **Note: DO NOT save any changes on the file.**		
36.	CA closes the KSR contents window and the file system window.		

Execute KSR signer

Step	Activity	Initials	Time
37.	CA identifies the KSR to be signed and runs, in the terminal window **`ksrsigner Kjqmt7v /media/KSR2048/ksr-root-2016-q4-0.xml`**		
38.	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 and 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
39.	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to identify him/herself, present identification document for IW1 to retain and read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN. IW1 enters RZM representative's name here: _____		
40.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?		
41.	CA then enters **"y"** in response to **"Is this correct y/n?"** to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in **/media/KSR2048/skr-root-2016-q4-0.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
42.	CA prints out a sufficient number of copies for participants using **`for i in $(seq X); do printlog ksrsigner-20160811-*.log; done`** where ksrsigner-**20160811**-*.log is replaced by log output file displayed by program. This example generates **X** copies and hands copies to participants.		
43.	IW1 attaches a copy to his/her script and writes **"KSR 2048"**		

Backup Newly Created SKR

Step	Activity	Initials	Time
44.	CA copies the contents of the KSR FD by running **`cp –p /media/KSR2048/* .`** for posting back to RZM. Confirm overwrite by entering "y" when prompted.		
45.	CA lists contents of KSR FD which should now have an SKR by running **`ls –ltr /media/KSR2048`** flushes the system buffers: **`sync`** and then unmounts the KSR FD using **`umount /media/KSR2048`**		
46.	CA removes the FD **KSR2048** containing SKR and gives it to the RZM representative.		

Insert 2nd KSR to be signed

Step	Activity	Initials	Time
47.	CA plugs FD labeled **"KSR1024FB"** with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA shows the KSR file contents by: a) Double click file b) Select **DISPLAY** on the pop-up menu c) Maximize the window to show the contents **Note: DO NOT save any changes on the file.**		
48.	CA closes the KSR contents window and the file system window.		

Execute KSR signer

Step	Activity	Initials	Time
49.	CA identifies the KSR to be signed and runs, in the terminal window **`ksrsigner Kjqmt7v /media/KSR1024FB/ksr-root-2016-q4-fallback-1.xml`**		
50.	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 and 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
51.	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to read out the SHA256 hash in PGP wordlist format for the KSR previously sent to ICANN.		
52.	Participants match the hash read out with that displayed on the terminal. CA asks, "are there any objections"?		
53.	CA then enters **`"y"`** in response to **`"Is this correct y/n?"`** to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in **`/media/KSR1024FB/skr-root-2016-q4-fallback-1.xml`**		

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
54.	CA prints out a sufficient number of copies for participants using **`for i in $(seq X); do printlog $(ls -tr ksrsigner-20160811-*.log | tail -n 1); done`** This example generates **X** copies and hands copies to participants.		
55.	IW1 attaches a copy to his/her script and writes **"KSR 1024 FallBack"**		

Backup Newly Created SKR

Step	Activity	Initials	Time
56.	CA copies the contents of the KSR FD by running **`cp -p /media/KSR1024FB/* .`** for posting back to RZM. Confirm overwrite by entering "y" when prompted.		
57.	CA lists contents of KSR FD which should now have an SKR by running **`ls -ltr /media/KSR1024FB`** flushes the system buffers: **`sync`** and then unmounts the KSR FD using **`umount /media/KSR1024FB`**		
58.	CA removes the FD **KSR1024FB** containing SKR and gives it to the RZM representative.		

Disable/Deactivate HSM

Step	Activity	Initials	Time
59.	CA makes sure to utilize the cards that were NOT used to activate the HSM are used to deactivate the HSM. CA will perform the following steps to deactivate the HSM: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"2.Set Offline"** hit **ENT** to confirm c) When **"Set Offline?"** is displayed, 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"** hit **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		

Act 3. Secure Hardware, Key Deletion and Zeroization the Old HSMs

Return HSM4 to a TEB

Step	Activity	Initials	Time
1.	CA switches the power OFF and disconnects HSM from power and laptop (serial and Ethernet) if connected.		
2.	CA places the HSM into a prepared TEB and seals it.		
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM4: TEB# BB24646625 / serial # H1411006** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.		

Restart Serial Port Activity

Step	Activity	Initials	Time
4.	CA switches to the ttyaudit terminal window and disconnects the USB serial adaptor from laptop. CA then re-connects the serial to USB null modem cable to the laptop.		
5.	CA executes the following to start logging of the HSM serial port outputs. `ttyaudit /dev/ttyUSB0` Note: **DO NOT** unplug the USB serial port from the laptop as this will cause logging to stop.		

Power Up HSM1

Step	Activity	Initials	Time
6.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM1: TEB# BB24646605 / serial # K6002020**		
7.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		
8.	CA connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp). **HSM1: serial # K6002020** **Note: The HSM date and time was set from the factory.**		

SO Cards

Step	Activity	Initials	Time
9.	One by one, CA calls each COs listed below to inspect their TEB for tamper evidence, opens the TEB and hands the SO cards to the CA who places the cards in cardholder visible to all. **CO 1: Arbogast Fabian** **SO TEB # BB46584262** **CO 2: Dmitry Burkov** **SO TEB # BB46584256** **CO 4: Carlos Martinez** **SO TEB # BB46584254** **CO 5: Olafur Gudmundsson** **SO TEB # BB46584252** **CO 6: Nicolas Antoniello** **SO TEB # BB46584284** **CO 7: Subramanian Moonesamy** **SO TEB # BB46584258**		

HSM1: List the KSK

Step	Activity	Initials	Time
10.	CA utilizes **3 SO cards** from **Set 1** to list the KSK stored on the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"4.Output Key Summary"** hit **ENT** to confirm i) When **"Key Summary?"** is displayed, hit **ENT** to confirm j) Select **"5.Output Key Details"** hit **ENT** to confirm k) When **"List Key?"** is displayed, hit **ENT** to confirm l) Hit **CLR** to return to the previous menu CA matches the displayed KSK label **`Kjqmt7v`** in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

HSM1: Delete the KSK

Step	Activity	Initials	Time
11.	CA utilizes **3 SO cards** from **Set 1** that were NOT used before to delete the KSK from the **HSM**: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"5.Key Mgmt"** hit **ENT** to confirm c) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"2.App Keys"** hit **ENT** to confirm i) Select **"7.Erase App Keys"** hit **ENT** to confirm j) When **"Erase App Keys?"** is displayed, hit **ENT** to confirm k) When **"Done"** is displayed, hit **ENT** to confirm l) Select **"4.Output Key Summary"** hit **ENT** to confirm m) When **"Key Summary?"** is displayed, hit **ENT** to confirm n) Select **"5.Output Key Details"** hit **ENT** to confirm o) When **"List Key?"** is displayed, hit **ENT** to confirm p) Hit **CLR** to return to the previous menu CA confirms there is not a key displayed in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

HSM1: Zeroization

Step	Activity	Initials	Time
12.	CA utilizes **3 SO cards** from **Set 2** to place the HSM on "**Initialized**" state. This will zeroise the HSM that will erase all keys (AAK, SMK, APP), settings and configuration: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"4.HSM Mgmt"** hit **ENT** to confirm c) When **"HSM Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"A.Go Initialised"** hit **ENT** to confirm i) When **"Go Initialised?"** is displayed, hit **ENT** to confirm j) Wait until **"Done"** is displayed. When this operation is complete the HSM will reboot and display **"Important Read Manual"** indicating that the HSM is in the initialized state. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 2 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

Return HSM1 to a TEB

Step	Activity	Initials	Time
13.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected.		
14.	CA places the HSM into a prepared TEB and seals it.		
15.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM1: TEB# BB24646623 / serial # K6002020** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.		

Power Up HSM2

Step	Activity	Initials	Time
16.	CA inspects the HSM TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 confirms TEB # and serial # below. **HSM2: TEB# BB24646669 / serial # K6002018**		
17.	CA removes HSM from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.		
18.	CA connects power to HSM. Status information should appear on the serial logging screen. IW1 matches displayed HSM serial number with below. (Time and date in the HSM may not match the time used for the ceremony logs, but there is no need to change it because the laptop does the script logging and timestamp.) **HSM2: serial # K6002018** **Note: The HSM date and time was set from the factory.**		

HSM2: List the KSK

Step	Activity	Initials	Time
19.	CA utilizes **3 SO cards** from **Set 2** that were NOT used before to list the KSK from the **HSM**: m) Utilize the HSM's keyboard and scroll through menu using <> key n) Select **"5.Key Mgmt"** hit **ENT** to confirm o) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm p) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder q) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** r) When "**Remove Card?"** is displayed, remove card s) Repeat steps d) to f) for the 2nd and 3rd SO card t) Select **"4.Output Key Summary"** hit **ENT** to confirm u) When **"Key Summary?"** is displayed, hit **ENT** to confirm v) Select **"5.Output Key Details"** hit **ENT** to confirm w)When **"List Key?"** is displayed, hit **ENT** to confirm x) Hit **CLR** to return to the previous menu CA matches displayed KSK keypair label **`Kjqmt7v`** in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 2 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

HSM2: Delete the KSK

Step	Activity	Initials	Time
20.	CA utilizes **3 SO cards** from **Set 1** to delete the KSK from the **HSM**: q) Utilize the HSM's keyboard and scroll through menu using <> key r) Select **"5.Key Mgmt"** hit **ENT** to confirm s) When **"Key Mgmt?"** is displayed, hit **ENT** to confirm t) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder u) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** v) When "**Remove Card?"** is displayed, remove card w) Repeat steps d) to f) for the 2nd and 3rd SO card x) Select **"2.App Keys"** hit **ENT** to confirm y) Select **"7.Erase App Keys"** hit **ENT** to confirm z) When **"Erase App Keys?"** is displayed, hit **ENT** to confirm aa) When **"Done"** is displayed, hit **ENT** to confirm bb) Select **"4.Output Key Summary"** hit **ENT** to confirm cc) When **"Key Summary?"** is displayed, hit **ENT** to confirm dd) Select **"5.Output Key Details"** hit **ENT** to confirm ee) When **"List Key?"** is displayed, hit **ENT** to confirm ff) Hit **CLR** to return to the previous menu CA confirms there is not a key displayed in the ttyaudit terminal window. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 1 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

HSM2: Zeroization

Step	Activity	Initials	Time
21.	CA utilizes **3 SO cards** from **Set 2** to place the HSM on "**Initialized**" state. This will zeroise the HSM that will erase all keys (AAK, SMK, APP), settings and configuration: a) Utilize the HSM's keyboard and scroll through menu using <> key b) Select **"4.HSM Mgmt"** hit **ENT** to confirm c) When **"HSM Mgmt?"** is displayed, hit **ENT** to confirm d) When **"Insert Card SO #?"** is displayed, insert the SO card from the cardholder e) When **"PIN?"** is displayed, enter **"11223344"** and hit **ENT** f) When "**Remove Card?"** is displayed, remove card g) Repeat steps d) to f) for the 2nd and 3rd SO card h) Select **"A.Go Initialised"** hit **ENT** to confirm i) When **"Go Initialised?"** is displayed, hit **ENT** to confirm j) Wait until **"Done"** is displayed. It may take a few minutes for HSM to restart after erasing all keys. When this operation is complete the HSM will reboot and after self test the HSM display should say **"Important Read Manual"** indicating the HSM is in the initialized state. IW1 records the used cards below. Each card is returned to cardholder after use. Set # 2 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7		

Act 4. Secure Hardware and Close the Ceremony

Return HSM2 to a TEB

Step	Activity	Initials	Time
1.	CA disconnects HSM from power and laptop (serial and Ethernet) if connected.		
2.	CA places the HSM into a prepared TEB and seals it.		
3.	CA reads out TEB # and HSM serial #, shows item to participants and IW1 confirms TEB # and HSM serial # below. **HSM2: TEB# BB24646624 / serial # K6002018** CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on 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 laptop. CA then exits out of **ttyaudit terminal window** by typing "exit".		
5.	**Terminating the logging script** CA stops logging terminal output by entering "exit" in the other terminal window. This only stops the script logging and will **NOT** close window.		

Backup HSMFD Contents

Step	Activity	Initials	Time
6.	CA sets dotglob by executing **`shopt -s dotglob`** This allows copying everything in the original HSMFD.		
7.	CA calculates the sha256hash of the contents on the original HSMFD. **`find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha256sum`**		
8.	CA copy and paste the sha256hash and paste it on Text Editor by going to **Applications > Accessories > Text Editor**		
9.	CA prints two copies of the hash. One for the audit bundle and the other for the HSMFD package then writes **"KSK 26"** on the printed copies.		
10.	CA displays contents of HSMFD by executing **`ls -ltr`**		
11.	CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the O/S (as HSMFD_); and copies the contents of the HSMFD to the blank drive for backup by executing **`cp -Rp * /media/HSMFD_`**		
12.	CA displays contents of HSMFD_ by executing **`ls -ltr /media/HSMFD_`**		
13.	Calculate the sha256hash of the contents on the copied HSMFD. **`find -P /media/HSMFD_ -type f -print0 | sort -z | xargs -0 cat | sha256sum`** Confirm that it matches the sha256hash of the original HSMFD by using the text editor to copy and paste the hash for comparison.		
14.	CA unmounts new FD using **`umount /media/HSMFD_`**		
15.	CA removes **HSMFD_** and places it on the table.		
16.	CA repeats step 11 to 15 for the 2nd copy		
17.	CA repeats step 11 to 15 for the 3rd copy		
18.	CA repeats step 11 to 15 for the 4th copy		
19.	CA repeats step 11 to 15 for the 5th copy		

Print Logging Information

Step	Activity	Initials	Time
20.	CA prints out a hard copy of logging information by executing **`enscript -2Gr -# 1 script-20160811.log`** **`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-20160811-*.log`** for attachment to IW1 script. **Note: Ignore the error regarding non-printable characters if prompted.**		

Returning HSMFD and O/S DVD to a TEB

Step	Activity	Initials	Time
21.	CA unmounts HSMFD by executing **`cd /tmp`** then **`umount /media/HSMFD`** CA removes HSMFD.		
22.	After all print jobs are complete, CA a) Turns off the laptop by pressing the power switch b) Turns on the laptop by pressing the power switch and immediately remove the O/S DVD from the laptop DVD drive c) Turns off the laptop again by pressing the power switch		
23.	CA places **TWO** HSMFDs and two OS/DVD, paper with printed hash in prepared TEB; and seals; reads out TEB #; shows item to participants and IW1 confirms TEB # below. **O/S DVD (release 20160503) + HSMFD: TEB# BB46584720**		
24.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.		

Distribute HSMFDs

Step	Activity	Initials	Time
25.	Remaining HSMFDs are distributed to IW1 (2 for audit bundles, 2 for IKOS) to post SKR to RZM, and to review, analyze and improve on procedures.		

Returning Laptop to a TEB

Step	Activity	Initials	Time
26.	CA disconnects printer, display, power, and any other connections from laptop and puts laptop in prepared TEB and seals; reads out TEB #, serial # laptop # and shows item to participants and IW1 confirms TEB #, serial # laptop # below. **Laptop1 (Dell ATG6400): TEB# BB24646622 / serial # 37240147333**		
27.	CA and IW1 initials the TEB using a ballpoint pen and keeps the sealing strips for later inventory. CA then places the TEB on equipment cart.		

Returning OP and SO Cards to TEBs

Step	Activity	Initials	Time
28.	CA calls each COs to the front of the room one at a time and repeats the steps below. a) CA takes the two TEBs prepared for the CO and reads out the TEB # and description while showing each bag. b) CO places his/her OP card into the plastic case. c) CO places his/her SO cards into the plastic case. d) CA places each plastic case into the proper TEBs, seals and initials TEB using a ballpoint pen. e) IW1 inspects each TEB, confirms description in the table on the next page and initials TEB using a ballpoint pen. IW1 keeps sealing strips for later inventory. f) CA hands each TEBs containing the OP and the SO cards to the CO. CO inspects and verifies TEB # and contents then initials his/her TEB using a ballpoint pen. g) CO enters completion time and signs for each TEB in the table below in IW1's script. IW1 initials table entry. h) CO returns to his/her seat with the TEBs, being careful not to poke or puncture TEBs. **CO 1: Arbogast Fabian** **OP TEB # BB46584657** **SO TEB # BB46584663** **CO 2: Dmitry Burkov** **OP TEB # BB46584658** **SO TEB # BB46584652** **CO 4: Carlos Martinez** **OP TEB # BB46584659** **SO TEB # BB46584665** **CO 5: Olafur Gudmundsson** **OP TEB # BB46584660** **SO TEB # BB46584666** **CO 6: Nicolas Antoniello** **OP TEB # BB46584661** **SO TEB # BB46584667** **CO 7: Subramanian Moonesamy** **OP TEB # BB46584662** **SO TEB # BB46584668**		

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46584657	Arbogast Fabian		11 August 2016		
CO 1	SO 1 of 7	BB46584663	Arbogast Fabian		11 August 2016		
CO 2	OP 2 of 7	BB46584658	Dmitry Burkov		11 August 2016		
CO 2	SO 2 of 7	BB46584652	Dmitry Burkov		11 August 2016		
CO 4	OP 4 of 7	BB46584659	Carlos Martinez		11 August 2016		
CO 4	SO 4 of 7	BB46584665	Carlos Martinez		11 August 2016		
CO 5	OP 5 of 7	BB46584660	Olafur Gudmundsson		11 August 2016		
CO 5	SO 5 of 7	BB46584666	Olafur Gudmundsson		11 August 2016		
CO 6	OP 6 of 7	BB46584661	Nicolas Antoniello		11 August 2016		
CO 6	SO 6 of 7	BB46584667	Nicolas Antoniello		11 August 2016		
CO 7	OP 7 of 7	BB46584662	Subramanian Moonesamy		11 August 2016		
CO 7	SO 7 of 7	BB46584668	Subramanian Moonesamy		11 August 2016		


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
TO: SUBRAMANIAN MOONESAMY
BB46584257
BB46584257
AMPAC
innovation in action
MADE IN THE USA
STOCK #GCS0912
ampaconline.com
KEEPSAFE
CUT BELOW DOTTED LINE TO OPEN

Figure 2

Returning Equipment to Safe #1

Step	Activity	Initials	Time
29.	CA, IW1, SSC1 open safe room and enter with equipment cart.		
30.	SSC1 opens Safe #1 shielding combination from camera.		
31.	SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
32.	CA records return of **HSM1, HSM2 and HSM4** in next entry field of safe log with TEB # and HSM serial #, printed name, date, time, and signature. CA **CAREFULLY** places the HSMs into Safe #1 and IW1 initials the entry. **HSM1: TEB# BB24646623** **HSM2: TEB# BB24646624** **HSM4: TEB# BB24646625**		
33.	CA records return of **laptop** in next entry field of safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry. **Laptop1 (Dell ATG6400): TEB# BB24646622**		
34.	CA records return of **O/S DVD + HSMFD** in next entry field of safe log with TEB #, printed name, date, time, and signature; places the **O/S DVD + HSMFD** into Safe #1 and IW1 initials the entry. **O/S DVD (release 20160503) + HSMFD: TEB# BB46584720**		

Close Equipment Safe #1

Step	Activity	Initials	Time
35.	SSC1 makes an entry including printed name, date, time, signature and notes “closing safe” in the safe log. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
36.	SSC1 places log back in safe and locks Safe #1 (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.		
37.	IW1, CA, and SSC1 return to ceremony room with equipment cart closing the door behind them.		

Open Credential Safe #2

Step	Activity	Initials	Time
38.	After a one (1) minute delay, CA, IW1, SSC2, and COs enter the safe room. CA brings a flashlight and the CO brings their OP and SO cards (if applicable) in TEBs with them.		
39.	SSC2 opens Safe #2 while shielding combination from camera.		
40.	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating the opening of the safe. IW1 initials the entry. **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
41.	One by one, each COs along with the CA (using his/her common key): a) Open his/her respective safe deposit box and read out box number inside Safe #2. **# Common Key is bottom lock and CO Key is top lock** b) CO makes an entry into the safe log indicating the return of OP card and SO cards (if applicable) including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB #s and card type to his/her script. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** c) CO shows each TEB to the camera and then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA. Repeat the steps above until all cards are returned to the deposit box. **CO 1: Arbogast Fabian** **Box #: 1791** **OP TEB # BB46584657** **SO TEB # BB46584663** **CO 2: Dmitry Burkov** **Box #: 1793** **OP TEB # BB46584658** **SO TEB # BB46584652** **CO 4: Carlos Martinez** **Box #: 1068** **OP TEB # BB46584659** **SO TEB # BB46584665** **CO 5: Olafur Gudmundsson** **Box #: 1789** **OP TEB # BB46584660** **SO TEB # BB46584666** **CO 6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584661** **SO TEB # BB46584667** **CO 7: Subramanian Moonesamy** **Box #: 1792** **OP TEB # BB46584662** **SO TEB # BB46584668**		

Close Credential Safe #2

Step	Activity	Initials	Time
42.	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "Close safe" into the safe log. IW1 initials the entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**		
43.	SSC2 puts log back in safe and locks Safe #2 (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.		
44.	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
45.	One by one, all participants come to the front of the room, confirms printed name and date. **Then, the participant declares that this script is a true and accurate record of the ceremony by signing on IW1's script coversheet.** IW1 records the completion time once all participants have signed the coversheet. **Note: If entry is pre-printed, verify the entry and sign.**		
46.	CA reviews IW1's script and signs it.		

Online Streaming Stops

Step	Activity	Initials	Time
47.	CA acknowledges the participation of online participants and confirms with SA to stop online streaming.		

Signing Out of Ceremony Room

Step	Activity	Initials	Time
48.	IKOS 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.		

Filming Stops

Step	Activity	Initials	Time
49.	CA confirms with SA to stop filming.		

Copying and Storing the Script

Step	Activity	Initials	Time
50.	IW1 makes at least 1 copy of his/her script for off-site audit bundle. Audit bundles each contain: 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 **02/11/2016 – 08/11/2016**) e) The IW1 attestation (A.1 below) f) SA attestation (A.2, A.3 below) All in a TEB labeled **"Root DNSSEC KSK Ceremony 26"**, 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 and Intrusion Detection System (SA1)
One electronic copy (physical flash drive) of the firewall configuration, the screenshots from the PAC-IDS configuration review, the list of the 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.

Owen Smigelski

_____

Date: 11 August 2016

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 February 2016 00:00 UTC** to now.

Connor Barthold

_____

Date: 11 August 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: 11 August 2016