Root DNSSEC KSK Ceremony 32

Wednesday February 7, 2018

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

This ceremony is executed under the DNSSEC Practice Statement for the Root Zone KSK Operator Version 4th Edition (2016-10-01)

Abbreviations

AUD =	Third Party Auditor	**CA =**	Ceremony Administrator	**CO =**	Crypto Officer
EW =	External Witness	**FD =**	Flash Drive	**HSM =**	Hardware Security Module
IW =	Internal Witness	**KMF =**	Key Management Facility	**KSR =**	Key Signing Request
OP =	Operator	**PTI =**	Public Technical Identifiers	**RKSH =**	Recovery Key Share Holder
RKOS =	RZ KSK Operations Security	**RZM =**	Root Zone Maintainer	**SA =**	System Administrator
SKR =	Signed Key Response	**SMK =**	Storage Master Key	**SO =**	Security Officer
SSC =	Safe Security Controller	**SW =**	Staff Witness	**TCR =**	Trusted Community Representative

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

Participants

Key Ceremony roles are found on https://www.iana.org/help/key-ceremony-roles

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

Title / Roles	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		8 February 2018	00:11
IW1	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO3	Joao Damas			
CO4	Carlos Martinez			
CO5	Olafur Gudmundsson			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Alejandro Bolivar / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Victor kao / RSM			
AUD	Chris Koucheki / RSM			
SA1	Connor Barthold / ICANN			
SA2	Mike Brennan / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Jennifer Johnson / PTI			
SW	James Cole / ICANN			
SW	Audrey Fery-Forgues / ICANN			
EW	William Turton			
EW	Nathan Anderson			
EW	Matthew Justus			

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

Note: The CA leads the ceremony. Dual Occupancy is enforced. Only CAs, IWs, or SAs can enter and escort other participants to the Ceremony room. Only CA + IW can enter the safe room and escort other participants. CAs, IWs, or SAs may escort participants out of the ceremony room at the CA's discretion and only when an IW + CA or SA remain inside the ceremony. No one may leave the Ceremony room if the safe room is occupied. All participants are required to sign in and out of the ceremony room using the visitor log. The SA starts filming before the participants enter the ceremony room.

Some steps during the ceremony may require the participants to tell and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the phonetic alphabet shown below must be used:

A	Alfa	AL-FAH
B	Bravo	BRAH-VOH
C	Charlie	CHAR-LEE
D	Delta	DELL-TAH
E	Echo	ECK-OH
F	Foxtrot	FOKS-TROT
G	Golf	GOLF
H	Hotel	HOH-TEL
I	India	IN-DEE-AH
J	Juliet	JEW-LEE-ETT
K	Kilo	KEY-LOH
L	Lima	LEE-MAH
M	Mike	MIKE
N	November	NO-VEM-BER
O	Oscar	OSS-CAH
P	Papa	PAH-PAH
Q	Quebec	KEH-BECK
R	Romeo	ROW-ME-OH
S	Sierra	SEE-AIR-RAH
T	Tango	TANG-GO
U	Uniform	YOU-NEE-FORM
V	Victor	VIK-TAH
W	Whiskey	WISS-KEY
X	Xray	ECKS-RAY
Y	Yankee	YANG-KEY
Z	Zulu	ZOO-LOO
1	One	WUN
2	Two	TOO
3	Three	TREE
4	Four	FOW-ER
5	Five	FIFE
6	Six	SIX
7	Seven	SEV-EN
8	Eight	AIT
9	Nine	NIN-ER
0	Zero	ZEE-RO

Act 1. Initiate Ceremony and Retrieve Equipment

Sign into the Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.	Y.G.	21:20
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the participants list on Page 2.	Y.G.	21:20

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	Y.G.	21:21
4.	CA explains the use of personal electronic devices during ceremony.	Y.G.	21:21
5.	CA briefly explains the purpose of the ceremony.	Y.G.	21:22

Verify the Time and Date

Step	Activity	Initials	Time
6.	IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2018/02/07 21:23 All entries into this script or any logs should follow this common source of time.	Y.G.	21:23

Open the Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 brings a flashlight then escorts SSC2, COs into the safe room.	Y.G	21:25
8.	SSC2 opens Safe #2 while shielding the combination from the camera.	Y.G.	21:28
9.	SSC2 removes the existing safe log and shows the most recent page to the audit camera. SSC2 obtains the pre-printed safe log from IW1, then writes the date/time and signature on the safe log where "Open Safe" is indicated. IW1 verifies this entry, then initials it.	Y.G	21:29

COs Extract the Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10.	One by one, the selected CO retrieves the required OP TEB and SO TEB (if specified) by following the steps below a) With the assistance of the CA (and his/her common key), the CO opens her/his safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock** b) CO reads out the safe deposit box number, verifies its integrity, then removes his/her OP TEB and SO TEB c) CO reads out the TEB serial numbers, then verifies its integrity while showing it to the audit camera above. d) CO retains OP TEB and SO TEB (if specified below) then locks the box. e) CO writes the date/time and signature on the safe log where removal of their TEBs are indicated. f) IW1 verifies the completed safe log entries, then initials it. Repeat these steps until all required cards listed below are removed. **CO 1: Arbogast Fabian** **Box # 1791** OP TEB # **BB46584476 (Retain)** SO TEB # **BB46584451 (Check and Return)** **CO 2: Dmitry Burkov** **Box # 1793** OP TEB # **BB46584477 (Retain)** SO TEB # **BB46584453 (Check and Return)** **CO 3: Joao Damas** **Box # 1071** OP TEB # **BB46584454 (Retain)** SO TEB # **BB46584455 (Check and Return)** **CO 4: Carlos Martinez** **Box # 1068** OP TEB # **BB46584659 (Retain)** SO TEB # **BB46584665 (Check and Return)** **CO 5: Olafur Gudmundsson** **Box # 1789** OP TEB # **BB46584478 (Retain)** SO TEB # **BB46584666 (Check and Return)** **CO 6: Nicolas Antoniello** **Box # 1073** OP TEB # **BB46584479 (Retain)** SO TEB # **BB46584459 (Check and Return)** **CO 7: Subramanian Moonesamy** **Box # 1792** OP TEB # **BB46584480 (Retain)** SO TEB # **BB46584461 (Check and Return)**	Y.G	21:44

Close the Credential Safe #2

Step	Activity	Initials	Time
11.	Once all relevant deposit boxes are closed and locked, SSC2 writes the date/time and signature on the safe log where "Close Safe" is indicated. IW1 verifies this entry then initials it.	Y.G.	21:44
12.	SSC2 returns the safe log back in the Safe #2 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	Y.G.	21:45
13.	IW1, CA, SSC2, and COs leave the safe room with smart card TEBs, closing the door behind them.	Y.G.	21:46

Open Equipment Safe #1

Step	Activity	Initials	Time
14.	CA, IW1 and SSC1 enter the safe room with a cart.	Y.G.	21:46
15.	SSC1 opens Safe #1 while shielding the combination from the camera.	Y.G.	21:47
16.	SSC1 takes out the existing safe log and shows the most recent page to the audit camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 writes the date/time and signature on the safe log where "Open Safe" is indicated. IW1 verifies this entry then initials it.	Y.G.	21:48

Remove the Equipment from Safe #1

Step	Activity	Initials	Time
17.	CA extracts each equipment from the safe by following the steps below: a) CAREFULLY remove the equipment TEB from the safe. b) Read out the TEB serial number, then verify its integrity while showing it to the audit camera. c) Place equipment TEB on the cart as specified on the list below. d) Write the date/time and signature on the safe log where "**Remove**" is indicated. e) IW1 verifies the safe log entry, then initials it. HSM4: **TEB# BB51184612 / serial # H1411006 (Place on cart)** HSM3: **TEB# BB51184623 / serial # H1403033 (Check and Return)** Laptop1: **TEB# BB51184625 / serial # 37240147333 (Place on cart)** Laptop2: **TEB# BB24646591 / serial # 7292928457 (Check and Return)** OS DVD (release 20170403) + HSMFD: **TEB# BB46584481 (Place on cart)**	Y.G.	21:54

Close the Equipment Safe #1 and exit the Safe Room

Step	Activity	Initials	Time
18.	SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry then initials it.	Y.G.	21:54
19.	SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	Y.G.	21:55
20.	CA, SSC1 and IW1 leaves the safe room with the cart, closing the door behind them.	Y.G.	21:55

Act 2. Setup Equipment

Initial Setup

Step	Activity	Initials	Time
1.	CA prepares each equipment by following the steps below: a) Remove all equipment TEB from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read out the TEB # and the serial # (if applicable) while IW1 matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place it on its designated area on the ceremony table. HSM4: **TEB# BB51184612 / serial # H1411006** Laptop1: **TEB# BB51184625 / serial # 37240147333** OS DVD (release 20170403) + HSMFD: **TEB# BB46584481**	Y.G.	22:01
2.	CA boots the laptop by following the steps below. a) Connect the power supply, external display, USB printer cable and USB null modem cable into the laptop. b) Immediately insert the new **OS DVD release 20170403** after the laptop power is switched ON.	Y.G.	22:08
3.	CA sets up the laptop by following the steps below. a) Press "CTRL+ALT+F2" to get a console prompt and log in as **root**. b) Execute `system-config-display --noui` c) Execute `killall Xorg` d) Confirm that external display works. e) Log in as **root**	Y.G.	22:10

Step	Activity	Initials	Time
4.	CA confirms that the printer is connected then configures printer as default and prints test page by going to **System > Administration > Printing** And follow the steps below: a) Click the **New Printer** icon (left side), leave everything default, then click the button **Forward.** b) Under "Select Connection" choose the first device "**HP Laserjet xxxx**" then click the button **Forward.** **Note**: The xxxx is the Printer Model c) Select **HP** and click the button **Forward.** d) Under "Models" scroll up and select **"Laserjet"** then click the button **Forward.** e) Click the button **Apply** to finish. f) Under "Local Printers" from the left menu, select "**printer".** g) Click the button **"Make Default Printer"** and "**Print Test Page".** h) Close the printer setup windows.	Y.G.	22:12
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.	Y.G.	22:12
6.	CA updates the date and time on the laptop while referencing from the clock. On the laptop terminal window, CA executes: `date -s "20180207 HH:MM:00"` where **HH** is two-digit Hour, **MM** is two digit Minutes and **00** is Zero Seconds CA executes `date` using the Terminal window to confirm the date is properly configured.	Y.G.	22:14

Format and label the blank FDs

Step	Activity	Initials	Time

7.	CA plugs a new FD into the laptop, then waits for it to be recognized by the OS, closes the file system popup window and formats the drive by executing
	`df`
	to confirm the drive letter that is assigned to the blank USB drive (e.g. sda, sdb, sdc),
	`umount /dev/sda1`
	to unmount the drive (change drive letter and partition if necessary),
	`mkfs.vfat -n HSMFD -I /dev/sda1`
	to execute a FAT32 format and label it as HSMFD.
	CA unplugs the FD.
		Y.G.	22:16

8.	CA repeats step 7 for the 2nd blank FD	Y.G.	22:16
9.	CA repeats step 7 for the 3rd blank FD	Y.G.	22:17
10.	CA repeats step 7 for the 4th blank FD	Y.G.	22:18
11.	CA repeats step 7 for the 5th blank FD	Y.G.	22:18

Connect the HSMFD

Step	Activity	Initials	Time
12.	CA plugs the **ceremony 30** HSMFD into the USB slot on the laptop and waits for the OS to recognize it. CA displays the HSMFD contents to all participants then closes the file system window. IW1 places the unused HSMFD 30 to the FD holder.	Y.G.	22:20
13.	CA calculates the SHA-256 hash of the contents on the copied HSMFD by executing `hsmfd-hash -c` IW1 confirms that the result matches the SHA-256 hash of the HSMFD from the **Ceremony 30** annotated script. SHA-256 hash: 5f378217c62d0556dae2122c8dd32b89cf8d5167e4f9d3b512b79ab9bf2336c0 PGP Wordlist of the SHA-256 hash: PGP Words: eyetooth consensus miser bookseller southward clergyman adult escapade surmount tomorrow atlas Chicago optic sociable briefcase matchmaker stagehand microscope drunken graduate tonic Waterloo stapler positive atlas processor pupil proximate slingshot cannonball Christmas recipe **Note: CA will assign some participants to confirm the hash displayed on the TV screen while the rest confirms the hash from the ceremony script.**	Y.G.	22:23

Start the Terminal Session Logging

Step	Activity	Initials	Time
14.	CA changes the default directory to the HSMFD by executing `cd /media/HSMFD`	Y.G.	22:23
15.	CA executes `script script-20180207.log` to start a capture of terminal output.	Y.G	22:24

Start the HSM Output Logging

Step	Activity	Initials	Time

16.	CA opens a second terminal window and maximizes its size for visibility by going to **Applications > Accessories > Terminal.**
	Follow the additional steps to maximize the terminal window:
	a) Click the **View** menu and select **Zoom In.**
	b) Repeat the step above as necessary.
	and executes
	`cd /media/HSMFD`
	and executes
	`stty -F /dev/ttyUSB0 115200`
	`ttyaudit /dev/ttyUSB0`
	to start logging HSM serial port outputs. Note: **DO NOT** unplug USB serial port from laptop as this causes logging to stop.
		Y.G.	22:25

Power Up the HSM

Step	Activity	Initials	Time
17.	CA prepares the HSM by following the steps below: a) Plug the ttyUSB0 null modem serial cable to the back of the HSM. b) Connect the power to HSM and switch the power ON. Status information should appear on the serial logging screen. c) Scroll the logging screen up for IW1 to match the displayed HSM serial number with the information below. **HSM4: serial # H1411006** **Note: The date/time on the HSM is not used as a reference for logging and timestamp.**	Y.G.	22:27

Act 3. Activate HSM and Generate Signatures

Enable/Activate the HSM3

Step	Activity	Initials	Time
1.	One by one, CA calls each COs listed below to inspect the TEB for tamper evidence. With the help of the CA, the CO opens the TEB and hands the OP cards to the CA, then places it on the card holder visible to everyone. **CO 1: Arbogast Fabian** OP TEB # **BB46584476** **CO 2: Dmitry Burkov** OP TEB # **BB46584477** **CO 3: Joao Damas** OP TEB # **BB46584454** **CO 4: Carlos Martinez** OP TEB # **BB46584659** **CO 5: Olafur Gudmundsson** OP TEB # **BB46584478** **CO 6: Nicolas Antoniello** OP TEB # **BB46584479** **CO 7: Subramanian Moonesamy** OP TEB # **BB46584480**	YG	22:33
2.	CA activates the **HSM** by following the steps below: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, hit **ENT** to confirm. c) Insert the OP card, then hit **ENT** to confirm. d) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT.** e) When **"Remove Card?"** is displayed, remove the OP card. f) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW1 records the used cards below. Each card is returned to card holder after use. 1st OP card 1 of 7 2nd OP card 2 of 7 3rd OP card 3 of 7 **Note: If the smartcard is unreadable, gently wipe its metal contacts and try again.**	YG	22:36

Check the Network Connectivity Between Laptop and HSM4

Step	Activity	Initials	Time
3.	CA connects the HSM to the laptop using Ethernet cable in **LAN** port.	Y.G.	22:37
4.	CA switches to the terminal window and tests network connectivity between laptop and HSM by executing: `ping 192.168.0.2` and wait for responses. Ctrl-C to exit program.	Y.G	22:37

Insert the KSR FD

Step	Activity	Initials	Time
5.	CA plugs the FD labeled **"KSR"** then waits for it to be recognized by the OS. CA points out the KSR file that will be signed on each folder, then closes the file system window. **Note:** The KSR FD was transferred to the facility by the RKOS. It contains four KSRs. One is for the normal operation and three are for fallback scenarios.	Y.G.	22:41

Execute the KSR Signer for Phase D to E

Step	Activity	Initials	Time
6.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK32-0-D_to_E/ksr-root-2018-q2-0-d_to_e.xml`	Y.G.	22:42
7.	The KSR signer will provide the following prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters "y" to proceed.	Y.G.	22:43

Verify the KSR Hash

Step	Activity	Initials	Time
8.	When the program requests verification of the KSR hash, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room and provide documents for IW1 to review. b) RZM representative reads out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. c) IW1 retains the documents provided by the RZM representative and writes the name below: Alejandro Bolivar	Y.G.	22:45
9.	Participants match the hash displayed on the terminal window, then CA asks, "are there any objections?"	Y.G	22:45
10.	CA enters "y" in response to "`Is this correct y/n?`" to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK32-0-D_to_E/skr-root-2018-q2-0-d_to_e.xml`	Y.G.	22:46

VERISIGN™

12061 Bluemont Way
Reston, Va. 20190
T: 703-948-3200
F: 703-948-3857

Verisign.com

February 5th, 2018

To Whom It May Concern:

This is a letter of Verification of Employment for Alejandro A. Bolivar. Verisign, Inc. has employed Alejandro A. Bolivar full-time since September 8th, 1997, currently as a Sr. Engineer – CBO in our Product Operations organization.

As the global leader in domain names, Verisign powers the invisible navigation that takes people to where they want to go on the Internet. For more than 19 years, Verisign has operated the infrastructure for a portfolio of top-level domains that today includes .com, .net, .tv .edu, .gov, .jobs, .name, and .cc, as well as two of the world's 13 Internet root servers. Verisign's product suite also includes Distributed Denial of Service (DDoS) Protection Services and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit Verisign.com.

Verisign manages and protects the global domain name system (DNS) infrastructure for more than 113 million domain names and processes approximately 60 billion queries daily, while maintaining 100 percent operational accuracy and stability for more than a decade. Our services also help ensure that online businesses are as available as the Web itself.

Should you have further questions, please contact me at the number below.

Sincerely,

David Carney
HR Specialist | Verisign, Inc. | 703-948-4143 | dcarney@verisign.com

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200
f: 701-987-6543

verisign.com

07 February 2018

The SHA256 hash of the 2018 Q2 KSR file is:

ksr-root-2018-q2-0-d_to_e.xml:
90a97a7d7f89be26369715eb868fe0a5030817008eac8ddf005411188e916484

The PGP wordlist for the hash above is:

peachy passenger keyboard insincere lockup matchmaker
skydive caretaker Christmas mosquito backfield underfoot
necklace midsummer tapeworm paperweight acme antenna
banjo adroitness orca penetrate optic therapist aardvark
equation Athens borderline orca miracle flytrap Jupiter

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK32-0-D_to_E/ksr-root-2018-q2-0-d_to_e.xml (at Wed Feb  7 22:42:19 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824  20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824        20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824  20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-0-D_to_E/ksr-root-2018-q2-0-d_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
90A97A7D7F89BE26369715EB868FE0A5030817008EAC8DDF005411188E916484
>> peachy passenger keyboard insincere lockup matchmaker skydive caretaker Christmas mosquito backfield underfoot ne
cklace midsummer tapeworm paperweight acme antenna banjo adroitness orca penetrate optic therapist aardvark equation
 Athens borderline orca miracle flytrap Jupiter <<

Reading KSK schedule "rollover(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/P,20326(Klajeyz)/S
3 19036(Kjqmt7v)/P,20326(Klajeyz)/S
4 19036(Kjqmt7v)/P,20326(Klajeyz)/S
5 19036(Kjqmt7v)/P,20326(Klajeyz)/S
6 19036(Kjqmt7v)/P,20326(Klajeyz)/S
7 19036(Kjqmt7v)/P,20326(Klajeyz)/S
8 19036(Kjqmt7v)/P,20326(Klajeyz)/S
9 19036(Kjqmt7v)/P,20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK32-0-D_to_E/skr-root-2018-q2-0-d_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824  20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570        20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570  20326(Klajeyz)/S,19036(Kjqmt7v)/P

SHA256 hash of SKR:
1AE1A163650F730FC636D654171F7904DBB9BA0944EEF5309D4B261BFC5B43DA
>> beehive tolerance ratchet Galveston fracture atmosphere hockey atmosphere southward congregate stockman equation
banjo businessman jawbone alkali suspense proximate shadow applicant crumpled universe vapor commando quadrant disab
le bookshelf bravado wayside exodus crucial surrender <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Execute the KSR Signer for Phase E to D

Step	Activity	Initials	Time
11.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK32-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml`	Y.G.	22:47
12.	The KSR signer will provide the following prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters "y" to proceed.	Y.G.	22:47

Verify the KSR Hash

Step	Activity	Initials	Time
13.	When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	Y.G	22:48
14.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	Y.G	22:48
15.	CA then enters `"y"` in response to `"Is this correct y/n?"` to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK32-1-E_to_D/skr-root-2018-q2-1-e_to_d.xml`	Y.G	22:48

Execute the KSR Signer for Phase D to D

Step	Activity	Initials	Time
16.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK32-2-D_to_D/ksr-root-2018-q2-2-d_to_d.xml`	Y.G.	22:49
17.	The KSR signer will provide the following prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters "y" to proceed.	Y.G.	22:49

Verify the KSR Hash

Step	Activity	Initials	Time
18.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	Y.G	22:50
19.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	Y.G.	22:50
20.	CA enters `"y"` in response to `"Is this correct y/n?"` to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK32-2-D_to_D/skr-root-2018-q2-2-d_to_d.xml`	Y.G.	22:50

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200
f: 701-987-6543

verisign.com

07 February 2018

The SHA256 hash of the 2018 Q2 KSR file is:

ksr-root-2018-q2-1-e_to_d.xml:
f9369c207830970fcfc558844464335b0555e0d22c9ec57feca9b4730b8cb837

The PGP wordlist for the hash above is:

waffle congregate python butterfat island commando
preshrunk atmosphere stagehand resistor endorse Jupiter
crumpled getaway chisel exodus adult equipment tapeworm
sensation Burbank onlooker solo integrate tumor passenger
scenic hurricane alone megaton select consensus

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK32-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml (at Wed Feb  7 22:47:24 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
F9369C207830970FCFC558844464335B0555E0D22C9EC57FECA9B4730B8CB837
>> waffle congregate python butterfat island commando preshrunk atmosphere stagehand resistor endorse Jupiter crumpl
ed getaway chisel exodus adult equipment tapeworm sensation Burbank onlooker solo integrate tumor passenger scenic h
urricane alone megaton select consensus <<

Reading KSK schedule "publish+(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/S,20326(Klajeyz)/P
3 19036(Kjqmt7v)/S,20326(Klajeyz)/P
4 19036(Kjqmt7v)/S,20326(Klajeyz)/P
5 19036(Kjqmt7v)/S,20326(Klajeyz)/P
6 19036(Kjqmt7v)/S,20326(Klajeyz)/P
7 19036(Kjqmt7v)/S,20326(Klajeyz)/P
8 19036(Kjqmt7v)/S,20326(Klajeyz)/P
9 19036(Kjqmt7v)/S,20326(Klajeyz)/P
Generated new SKR in /media/KSR/KSK32-1-E_to_D/skr-root-2018-q2-1-e_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
59D0EB6A60F6DB70C942C950222D063521307EC7E008F22C0C5FAAD156BBCFE3
>> endow savagery trouble hamburger facial vocalist suspense hesitate spearhead December spearhead embezzle blockade
 clergyman afflict conformist blackjack commando locale retraction tapeworm antenna uproot Chicago ammo forever rewa
rd scavenger egghead publisher stagehand torpedo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200
f: 701-987-6543

verisign.com

07 February 2018

The SHA256 hash of the 2018 Q2 KSR file is:

ksr-root-2018-q2-2-d_to_d.xml:
b3b574377b61ac98e06628a15aed784368e50b9bf80a8380f174b7511ea07ff5

The PGP wordlist for the hash above is:

scallion positive indoors consensus kickoff frequency
ribcage narrative tapeworm gossamer breadline outfielder
enlist unify island decimal frighten travesty alone
Norwegian Vulcan Apollo Mohawk intention unwind hydraulic
seabird enchanting berserk Orlando lockup visitor

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK32-2-D_to_D/ksr-root-2018-q2-2-d_to_d.xml (at Wed Feb  7 22:49:20 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-2-D_to_D/ksr-root-2018-q2-2-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
B3B574377B61AC98E06628A15AED784368E50B9BF80A8380F174B7511EA07FF5
>> scallion positive indoors consensus kickoff frequency ribcage narrative tapeworm gossamer breadline outfielder en
list unify island decimal frighten travesty alone Norwegian Vulcan Apollo Mohawk intention unwind hydraulic seabird
enchanting berserk Orlando lockup visitor <<

Reading KSK schedule "publish+(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/S,20326(Klajeyz)/P
3 19036(Kjqmt7v)/S,20326(Klajeyz)/P
4 19036(Kjqmt7v)/S,20326(Klajeyz)/P
5 19036(Kjqmt7v)/S,20326(Klajeyz)/P
6 19036(Kjqmt7v)/S,20326(Klajeyz)/P
7 19036(Kjqmt7v)/S,20326(Klajeyz)/P
8 19036(Kjqmt7v)/S,20326(Klajeyz)/P
9 19036(Kjqmt7v)/S,20326(Klajeyz)/P
Generated new SKR in /media/KSR/KSK32-2-D_to_D/skr-root-2018-q2-2-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
759EAB97E71C95A518C6099EC5E4A4FBAAC7162DF2C381E6888EDF7857CB687D
>> indulge onlooker rhythm mosquito transit Brazilian preclude paperweight beaming responsive Algol onlooker solo tr
adition regain Wichita reward retraction backward clergyman uproot replica minnow trombonist newborn microwave talon
 indigo eightball revival frighten insincere <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Execute the KSR Signer for Phase C to C

Step	Activity	Initials	Time
21.	CA uses the terminal window to sign the KSR file by executing the following: `ksrsigner /media/KSR/KSK32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml`	Y.G	22:50
22.	The KSR signer will provide the following prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters "y" to proceed.	Y.G.	22:51

Verify the KSR Hash

Step	Activity	Initials	Time
23.	When the program requests verification of the KSR hash, the CA asks the Root Zone Maintainer (RZM) representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	Y.G.	22:51
24.	Participants match the hash read out displayed on the terminal window. CA asks, "are there any objections"?	Y.G.	22:51
25.	CA enters `"y"` in response to `"Is this correct y/n?"` to complete the KSR signing operation. The SKR is located on `/media/KSR/KSK32-3-C_to_C/skr-root-2018-q2-3-c_to_c.xml`	Y.G	22:51

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
26.	CA prints out sufficient number of copies for participants by executing the following command on the terminal window `for i in $(ls -1 ksrsigner-20180207*.log); do printlog $i X; done` **Note:** Replace **X** with the number of copies for the participants.	Y.G	22:58
27.	IW1 attaches a copy of each ksrsigner log to his/her script.	Y.G	22:58

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200
f: 701-987-6543

verisign.com

07 February 2018

The SHA256 hash of the 2018 Q2 KSR file is:

ksr-root-2018-q2-3-c_to_c.xml:
b7718ecc5c95e29a96e991f54bce9808f859e7e1bb3d966137026 1f6fc6f4721

The PGP wordlist for the hash above is:

seabird hideaway orca revolver escape Montana tiger
newsletter prefer ultimate pheasant visitor dragnet
sardonic printer antenna Vulcan examine transit tolerance
shamrock crucifix prefer frequency clamshell aftermath
fallout vocalist wayside hemisphere dashboard Camelot

Attested on behalf of VeriSign by:

Alejandro Bolivar
Senior Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml (at Wed Feb  7 22:50:53 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception            Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml...
#  Inception            Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
B7718ECC5C95E29A96E991F54BCE9808F859E7E1BB3D9661370261F6FC6F4721
>> seabird hideaway orca revolver escape Montana tiger newsletter prefer ultimate pheasant visitor dragnet sardonic
printer antenna Vulcan examine transit tolerance shamrock crucifix prefer frequency clamshell aftermath fallout voca
list wayside hemisphere dashboard Camelot <<

Reading KSK schedule "normal(2010)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
2 19036(Kjqmt7v)/S
3 19036(Kjqmt7v)/S
4 19036(Kjqmt7v)/S
5 19036(Kjqmt7v)/S
6 19036(Kjqmt7v)/S
7 19036(Kjqmt7v)/S
8 19036(Kjqmt7v)/S
9 19036(Kjqmt7v)/S
Generated new SKR in /media/KSR/KSK32-3-C_to_C/skr-root-2018-q2-3-c_to_c.xml
#  Inception            Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         19036(Kjqmt7v)/S
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         19036(Kjqmt7v)/S
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         19036(Kjqmt7v)/S
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         19036(Kjqmt7v)/S
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         19036(Kjqmt7v)/S
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         19036(Kjqmt7v)/S
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         19036(Kjqmt7v)/S
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   19036(Kjqmt7v)/S

SHA256 hash of SKR:
7A754353BE4AD3EAECD783FF895AEB22C74903571456B23EB2F94A86501C7BCB
>> keyboard impartial crucial enterprise skydive direction stapler undaunted tumor stethoscope Mohawk Yucatan nightb
ird existence trouble candidate soybean dinosaur acme Eskimo baboon escapade sawdust cumbersome sawdust Waterloo dog
sled letterhead drumbeat Brazilian kickoff revival <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Backup the Newly Created SKR

Step	Activity	Initials	Time
28.	CA copies the contents of the KSR FD by executing the following command on the terminal window `cp -pR /media/KSR/* .` Confirm overwrite by entering "y" if prompted.	Y.G.	22:59

29.	CA uses the terminal window to perform the following commands:
	a) list the contents of the KSR FD by executing
	`ls -ltrR /media/KSR`
	b) flush the system buffers by executing
	`sync`
	c) unmount the KSR FD by executing
	`umount /media/KSR`
		Y.G.	23:00

30.	CA removes the **KSR** FD containing the SKR files, then gives it to the RZM representative.	Y.G.	23:00

Disable/Deactivate the HSM

Step	Activity	Initials	Time
31.	CA ensures to utilize the unused cards to deactivate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Set Offline"**, then hit **ENT** to confirm. c) Insert the OP card, then hit **ENT** to confirm. d) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT.** e) When "**Remove Card?"** is displayed, remove the OP card. f) Repeat steps d) to e) for the 2nd and 3rd OP cards. Confirm that the **"READY"** LED on the HSM is **OFF.** IW1 records the used cards below. Each card is returned to card holder after use. 1st OP card 4 of 7 2nd OP card 5 of 7 3rd OP card 6 of 7 **Note: If the smartcard is unreadable, gently wipe its metal contacts and try again.**	Y.G.	23:03

Test the Unused OP Card

Step	Activity	Initials	Time
32.	CA tests the unused OP card's readability by following the steps below: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"8.View Cards"**, then hit **ENT** to confirm. c) Insert the OP card, then hit **ENT** to confirm. d) Verify that "OP" is displayed on the HSM, then hit **ENT** four times to display the information on the terminal window. e) Remove the OP card and return to the card holder. f) Hit **CLR** to return to the previous menu. IW1 records the used card below. OP card 7 of 7 **Note: If the smartcard is unreadable, gently wipe its metal contacts and try again.**	Y.G	23:05

Act 4. Secure Hardware

Return the HSM to TEB

Step	Activity	Initials	Time
1.	CA switches the HSM to power OFF, then disconnects the power and laptop (serial and Ethernet) connections from it. **Note: DO NOT** unplug the connections on the laptop end.	Y.G.	23:06
2.	CA places the HSM into a prepared TEB, then seals it.	Y.G.	23:07
3.	CA performs the following steps: a) Read out the TEB# and HSM serial #, then shows it to the audit camera above for participants to see. b) Confirm with IW1 that the TEB# and HSM serial # match below. c) Initial the TEB with IW1 using a ballpoint pen. d) Give IW1 the sealing strips for later inventory. e) Place the HSM TEB on the cart. **HSM4: TEB# BB51184642 / serial # H1411006**	Y.G.	23:09

Stop the Serial Port Activity and the Terminal Activity Logging

Step	Activity	Initials	Time
4.	CA performs the following steps to stop logging: a) Disconnect the USB serial adaptor from the laptop. b) Type "exit" then press enter on the Serial Port Activity (**ttyaudit**) window. c) Switch to the Terminal activity window. d) Type "exit" then press enter to stop logging. This window will remain open.	Y.G	23:11

Backup the HSMFD Contents

Step	Activity	Initials	Time
5.	CA sets dotglob by executing the command below on the terminal window `shopt -s dotglob` **Note:** This enables copying of all files from the original HSMFD.	Y.G.	23:11
6.	CA prints two copies of the hash by executing the following command on the terminal window twice: `hsmfd-hash -p` **Note:** One copy for audit bundle and one copy for HSMFD package.	Y.G.	23:12
7.	CA displays the contents of HSMFD by executing the following command on the terminal window `ls -ltrR`	Y.G.	23:12
8.	CA plugs a blank FD labeled HSMFD into a free USB slot on the laptop, then waits for the OS to recognize it as HSMFD_	Y.G.	23:13
9.	CA closes the file system window, then creates a backup of the HSMFD by executing following command on the terminal window `cp -pR * /media/HSMFD_`	Y.G.	23:14
10.	CA displays the contents of HSMFD_ by executing the following command on the terminal window `ls -ltrR /media/HSMFD_`	Y.G	23:14
11.	CA matches the SHA-256 hash between the original HSMFD and the copy HSMFD by executing the following command on the terminal window `hsmfd-hash -m`	Y.G.	23:15
12.	CA unmounts the HSMFD copy by executing the following command on the terminal window `umount /media/HSMFD_`	Y.G	23:15
13.	CA removes the **HSMFD_** and places it on the holder.	Y.G.	23:15
14.	CA repeats step 8 to 13 for the 2nd copy.	Y.G	23:17
15.	CA repeats step 8 to 13 for the 3rd copy.	Y.G.	23:18
16.	CA repeats step 8 to 13 for the 4th copy.	Y.G.	23:19
17.	CA repeats step 8 to 13 for the 5th copy.	Y.G.	23:20

Print Logging Information

Step	Activity	Initials	Time

18.	CA prints out a copy of the logging information by executing the following command on the terminal window
	`enscript -2Gr -# 1 script-201802*.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-201802*.log`
	Attach the printed copies to IW1 script.
	Note: Ignore the error regarding non-printable characters if prompted.
		Y.G.	23:22

HSMFD SHA-256 HASH **2018/02/07**

```
# find -P /media/HSMFD -type f -print0 | sort -z | xargs -0 cat | sha2wordlist

SHA-256:     e3d877c855ec3d1a1f97f07c397e7b75c208f0afa7ef65811b45396d5bb246fe
PGP Words:  tissue stupendous involve retrieval edict unicorn commence Bradbury billiar
d mosquito unearth informant classroom insurgent kickoff impartial snapshot antenna une
arth pharmacy repay unravel fracture inventive beeswax detector classroom hazardous era
se pioneer cubic yesteryear
```

```
Script started on Wed 07 Feb 2018 10:24:14 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=1.78 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.361 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.517 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.349 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=255 time=0.351 ms
64 bytes from 192.168.0.2: icmp_seq=6 ttl=255 time=0.351 ms
64 bytes from 192.168.0.2: icmp_seq=7 ttl=255 time=0.354 ms

--- 192.168.0.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6000ms
rtt min/avg/max/mdev = 0.349/0.580/1.783/0.495 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/KSR/KSK
32-0-D_to_E/k\007sr-root-2018-q2-0-d_to_e.xml
Starting: ksrsigner /media/KSR/KSK32-0-D_to_E/ksr-root-2018-q2-0-d_to_e.xml (at Wed Fe
b  7 22:42:19 2018 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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-0-D_to_E/ksr-root-2018-q2-0-d_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
90A97A7D7F89BE26369715EB868FE0A5030817008EAC8DDF005411188E916484
>> peachy passenger keyboard insincere lockup matchmaker skydive caretaker Christmas m
osquito backfield underfoot necklace midsummer tapeworm paperweight acme antenna banjo
 adroitness orca penetrate optic therapist aardvark equation Athens borderline orca mi
racle flytrap Jupiter <<
Is this correct (y/N)? y

Reading KSK schedule "rollover(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/P,20326(Klajeyz)/S
3 19036(Kjqmt7v)/P,20326(Klajeyz)/S
4 19036(Kjqmt7v)/P,20326(Klajeyz)/S
5 19036(Kjqmt7v)/P,20326(Klajeyz)/S
6 19036(Kjqmt7v)/P,20326(Klajeyz)/S
7 19036(Kjqmt7v)/P,20326(Klajeyz)/S
8 19036(Kjqmt7v)/P,20326(Klajeyz)/S
9 19036(Kjqmt7v)/P,20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK32-0-D_to_E/skr-root-2018-q2-0-d_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt
7v)/P

SHA256 hash of SKR:
1AE1A163650F730FC636D654171F7904DBB9BA0944EEF5309D4B261BFC5B43DA
>> beehive tolerance ratchet Galveston fracture atmosphere hockey atmosphere southward
 congregate stockman equation banjo businessman jawbone alkali suspense proximate shad
ow applicant crumpled universe vapor commando quadrant disable bookshelf bravado waysi
de exodus crucial surrender <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180207-224219.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/M033[KK
SR/KSK32\007-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml
Starting: ksrsigner /media/KSR/KSK32-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml (at Wed Fe
b  7 22:47:24 2018 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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-1-E_to_D/ksr-root-2018-q2-1-e_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
F9369C207830970FCFC558844464335B0555E0D22C9EC57FECA9B4730B8CB837
>> waffle congregate python butterfat island commando preshrunk atmosphere stagehand r
esistor endorse Jupiter crumpled getaway chisel exodus adult equipment tapeworm sensat
ion Burbank onlooker solo integrate tumor passenger scenic hurricane alone megaton sel
ect consensus <<
Is this correct (y/N)? y

Reading KSK schedule "publish+(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/S,20326(Klajeyz)/P
3 19036(Kjqmt7v)/S,20326(Klajeyz)/P
4 19036(Kjqmt7v)/S,20326(Klajeyz)/P
5 19036(Kjqmt7v)/S,20326(Klajeyz)/P
6 19036(Kjqmt7v)/S,20326(Klajeyz)/P
7 19036(Kjqmt7v)/S,20326(Klajeyz)/P
8 19036(Kjqmt7v)/S,20326(Klajeyz)/P
9 19036(Kjqmt7v)/S,20326(Klajeyz)/P
Generated new SKR in /media/KSR/KSK32-1-E_to_D/skr-root-2018-q2-1-e_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
59D0EB6A60F6DB70C942C950222D063521307EC7E008F22C0C5FAAD156BBCFE3
>> endow savagery trouble hamburger facial vocalist suspense hesitate spearhead Decemb
er spearhead embezzle blockade clergyman afflict conformist blackjack commando locale
retraction tapeworm antenna uproot Chicago ammo forever reward scavenger egghead publi
sher stagehand torpedo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180207-224724.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/K\033[K
\007SR/KSK32\007-2-D_to_D/ks\007k-r\007Y033[K033[K033[K033[Ksr-root-2018-q2-2-d_to_d.xm
l
Starting: ksrsigner /media/KSR/KSK32-2-D_to_D/ksr-root-2018-q2-2-d_to_d.xml (at Wed Fe
b  7 22:49:20 2018 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 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
```

```
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824    20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-2-D_to_D/ksr-root-2018-q2-2-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
B3B574377B61AC98E06628A15AED784368E50B9BF80A8380F174B7511EA07FF5
>> scallion positive indoors consensus kickoff frequency ribcage narrative tapeworm go
ssamer breadline outfielder enlist unify island decimal frighten travesty alone Norweg
ian Vulcan Apollo Mohawk intention unwind hydraulic seabird enchanting berserk Orlando
 lockup visitor <<
Is this correct (y/N)? y

Reading KSK schedule "publish+(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/S,20326(Klajeyz)/P
3 19036(Kjqmt7v)/S,20326(Klajeyz)/P
4 19036(Kjqmt7v)/S,20326(Klajeyz)/P
5 19036(Kjqmt7v)/S,20326(Klajeyz)/P
6 19036(Kjqmt7v)/S,20326(Klajeyz)/P
7 19036(Kjqmt7v)/S,20326(Klajeyz)/P
8 19036(Kjqmt7v)/S,20326(Klajeyz)/P
9 19036(Kjqmt7v)/S,20326(Klajeyz)/P
Generated new SKR in /media/KSR/KSK32-2-D_to_D/skr-root-2018-q2-2-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
759EAB97E71C95A518C6099EC5E4A4FBAAC7162DF2C381E6888EDF7857CB687D
>> indulge onlooker rhythm mosquito transit Brazilian preclude paperweight beaming res
ponsive Algol onlooker solo tradition regain Wichita reward retraction backward clergy
man uproot replica minnow trombonist newborn microwave talon indigo eightball revival
frighten insincere <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180207-224920.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsigner /media/KSR/KSK
32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml
Starting: ksrsigner /media/KSR/KSK32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml (at Wed Fe
b  7 22:50:53 2018 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 9860-2
    Serial:           H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-01-01T00:00:00 2018-01-22T00:00:00  46809,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-01-11T00:00:00 2018-02-01T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-01-21T00:00:00 2018-02-11T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-01-31T00:00:00 2018-02-21T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-02-10T00:00:00 2018-03-03T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-02-20T00:00:00 2018-03-13T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-03-02T00:00:00 2018-03-23T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-03-12T00:00:00 2018-04-02T00:00:00  41824         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-03-22T00:00:00 2018-04-12T00:00:00  39570,41824   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK32-3-C_to_C/ksr-root-2018-q2-3-c_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  41824,39570
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570
```

```
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570
9  2018-06-20T00:00:00 2018-07-11T00:00:00  39570,41656
...PASSED.

SHA256 hash of KSR:
B7718ECC5C95E29A96E991F54BCE9808F859E7E1BB3D9661370261F6FC6F4721
>> seabird hideaway orca revolver escape Montana tiger newsletter prefer ultimate phea
sant visitor dragnet sardonic printer antenna Vulcan examine transit tolerance shamroc
k crucifix prefer frequency clamshell aftermath fallout vocalist wayside hemisphere da
shboard Camelot <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2010)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
2 19036(Kjqmt7v)/S
3 19036(Kjqmt7v)/S
4 19036(Kjqmt7v)/S
5 19036(Kjqmt7v)/S
6 19036(Kjqmt7v)/S
7 19036(Kjqmt7v)/S
8 19036(Kjqmt7v)/S
9 19036(Kjqmt7v)/S
Generated new SKR in /media/KSR/KSK32-3-C_to_C/skr-root-2018-q2-3-c_to_c.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         19036(Kjqmt7v)/S
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         19036(Kjqmt7v)/S
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         19036(Kjqmt7v)/S
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         19036(Kjqmt7v)/S
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         19036(Kjqmt7v)/S
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         19036(Kjqmt7v)/S
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         19036(Kjqmt7v)/S
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   19036(Kjqmt7v)/S

SHA256 hash of SKR:
7A754353BE4AD3EAECD783FF895AEB22C74903571456B23EB2F94A86501C7BCB
>> keyboard impartial crucial enterprise skydive direction stapler undaunted tumor ste
thoscope Mohawk Yucatan nightbird existence trouble candidate soybean dinosaur acme Es
kimo baboon escapade sawdust cumbersome sawdust Waterloo dogsled letterhead drumbeat B
razilian kickoff revival <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180207-225053.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# for i in $(ls -1 ksrsign
er-\0072018\0070207-22033[K033[K033[K033[K7*.log); do printlog $i X033[K14; done
[ 1 pages * 14 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 14 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 14 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 14 copy ] sent to printer
2 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -pR /media/KSR/* .
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -ltrR /media/KSR/
\033[00m/media/KSR/:
total 16
drwxr-xr-x 2 root root 4096 Feb  7 22:45 \033[00;34mKSK32-0-D_to_E\033[00m
drwxr-xr-x 2 root root 4096 Feb  7 22:48 \033[00;34mKSK32-1-E_to_D\033[00m
drwxr-xr-x 2 root root 4096 Feb  7 22:50 \033[00;34mKSK32-2-D_to_D\033[00m
drwxr-xr-x 2 root root 4096 Feb  7 22:51 \033[00;34mKSK32-3-C_to_C\033[00m

/media/KSR/KSK32-0-D_to_E:
total 108
-rwxr-xr-x 1 root root 24928 Jan 29 18:58 \033[00;32mskr.xml.20180207224219\033[00m
-rwxr-xr-x 1 root root 19556 Jan 29 18:58 \033[00;32mksr-root-2018-q2-0-d_to_e.xml\033
[00m
-rwxr-xr-x 1 root root  1344 Jan 29 18:58 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Feb  7 22:45 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Feb  7 22:45 \033[00;32mskr-root-2018-q2-0-d_to_e.xml\033
[00m

/media/KSR/KSK32-1-E_to_D:
total 108
-rwxr-xr-x 1 root root 24928 Jan 29 18:58 \033[00;32mskr.xml.20180207224724\033[00m
-rwxr-xr-x 1 root root 19556 Jan 29 18:58 \033[00;32mksr-root-2018-q2-1-e_to_d.xml\033
[00m
-rwxr-xr-x 1 root root  1344 Jan 29 18:58 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Feb  7 22:48 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Feb  7 22:48 \033[00;32mskr-root-2018-q2-1-e_to_d.xml\033
[00m

/media/KSR/KSK32-2-D_to_D:
total 108
-rwxr-xr-x 1 root root 24928 Jan 29 18:58 \033[00;32mskr.xml.20180207224920\033[00m
-rwxr-xr-x 1 root root 19556 Jan 29 18:58 \033[00;32mksr-root-2018-q2-2-d_to_d.xml\033
[00m
-rwxr-xr-x 1 root root  1344 Jan 29 18:58 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Feb  7 22:50 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Feb  7 22:50 \033[00;32mskr-root-2018-q2-2-d_to_d.xml\033
[00m

/media/KSR/KSK32-3-C_to_C:
total 92
-rwxr-xr-x 1 root root 24928 Jan 29 18:58 \033[00;32mskr.xml.20180207225053\033[00m
-rwxr-xr-x 1 root root 19556 Jan 29 18:58 \033[00;32mksr-root-2018-q2-3-c_to_c.xml\033
[00m
-rwxr-xr-x 1 root root  1148 Jan 29 18:58 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 20347 Feb  7 22:51 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Feb  7 22:51 \033[00;32mskr-root-2018-q2-3-c_to_c.xml\033
[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# sync
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/KSR/
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit

Script done on Wed 07 Feb 2018 11:11:00 PM UTC
```

```
2018-02-07T22:26:44+0000        ttyUSB0 ûþÿ
2018-02-07T22:26:44+0000        ttyUSB0
2018-02-07T22:26:44+0000        ttyUSB0 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2018-02-07T22:26:44+0000        ttyUSB0
2018-02-07T22:26:44+0000        ttyUSB0 BBL CRC32: 0x757574CA
2018-02-07T22:26:44+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ####################################
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ###     ABL tamper records       ###
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ####################################
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ====================================
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 vextoosTamperCount:     0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 vintoosTamperCount:     10
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 vbboosTamperCount:      0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 maxstrtempTamperCount:  0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 minstrtempTamperCount:  0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 meshTamperCount:        0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 extampSMKTamperCount:   0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 extampIMKTamperCount:   0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 tempdiffTamperCount:    0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 pfTamperCount:          10
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 restartTamperCount:     34
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 Current tamper bitmaps:
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ======================
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
```

```
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0 ============================================
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:45+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0 Board is P2020RDB
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0 board_smp_init: 2 cpu
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:46+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2018-02-07T22:26:46+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0 Starting next program at v0015183c
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0 Starting K-Series Kernel
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0 Wed Feb  7 21:33:39 2018
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:47+0000        ttyUSB0 Starting auditd v2.0 ... started.
2018-02-07T22:26:47+0000        ttyUSB0
2018-02-07T22:26:48+0000        ttyUSB0 Interface 0 configured for IPv6.
2018-02-07T22:26:48+0000        ttyUSB0
2018-02-07T22:26:48+0000        ttyUSB0 Interface 0 configured for IPv4.
2018-02-07T22:26:48+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0 Starting USB driver...
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0
2018-02-07T22:26:49+0000        ttyUSB0
```

```
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 Running DES POST Test
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 DES POST Test Passed
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 Running Triple DES POST Test
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 Triple DES POST Test Passed
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 Running AES POST Test
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 AES POST Test Passed
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 Running SHA1 POST Test
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 SHA1 POST Test Passed
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 Running SHA2 POST Test
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:50+0000        ttyUSB0 SHA2 POST Test Passed
2018-02-07T22:26:50+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 Running RandomGen POST Test
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 RandomGen POST Test Passed
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 Running RSA POST Test
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 RSA POST Test Passed
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 Running DSA POST Test
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 DSA POST Test Passed
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 Running ECC POST Test
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 ECC POST Test Passed
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0 Audit on 7/2/2018 21:33:42 00100008
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:51+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 Keyper 9860-2  Serial Number H1411006
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 Memory Usage:
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 RAM (free/total)        197Mb/256Mb
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0    black store          472b
```

```
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0    statistics           112b
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0    other                116b
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 RedStore (free/total)   109Kb/128Kb
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 Network Configuration:
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 IPv4: enabled
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 IPv6: enabled
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B3:1B / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b31b/64
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 HSM Port: 05000
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 Software Versions:
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 BBL 010 ABL 011 App 023
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 CPLD Version:
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 1.9
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 SCR Firmware Version:
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 OROS-R2.99-R1.20
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:26:52+0000        ttyUSB0 Audit on 7/2/2018 21:33:43 00100003
2018-02-07T22:26:52+0000        ttyUSB0
2018-02-07T22:34:53+0000        ttyUSB0 Audit on 7/2/2018 21:41:44 00200069 0A400000B706296E
2018-02-07T22:34:53+0000        ttyUSB0
2018-02-07T22:35:48+0000        ttyUSB0 Audit on 7/2/2018 21:42:39 00200069 0A4000009D06296E
2018-02-07T22:35:48+0000        ttyUSB0
```

```
2018-02-07T22:36:16+0000        ttyUSB0 Audit on 7/2/2018 21:43:07 00200069 0A400000B646296E
2018-02-07T22:36:16+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0 TcpListener: Created IPv4 socket 14 on port 5000.
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0 TcpListener: Created IPv6 socket 15 on port 5000.
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:36:18+0000        ttyUSB0 Audit on 7/2/2018 21:43:10 00100002
2018-02-07T22:36:18+0000        ttyUSB0
2018-02-07T22:42:47+0000        ttyUSB0
2018-02-07T22:42:47+0000        ttyUSB0
2018-02-07T22:42:47+0000        ttyUSB0 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2018-02-07T22:42:47+0000        ttyUSB0
2018-02-07T22:45:53+0000        ttyUSB0
2018-02-07T22:45:53+0000        ttyUSB0
2018-02-07T22:45:53+0000        ttyUSB0 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2018-02-07T22:45:53+0000        ttyUSB0
2018-02-07T22:47:35+0000        ttyUSB0
2018-02-07T22:47:35+0000        ttyUSB0
2018-02-07T22:47:35+0000        ttyUSB0 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2018-02-07T22:47:35+0000        ttyUSB0
2018-02-07T22:48:29+0000        ttyUSB0
2018-02-07T22:48:29+0000        ttyUSB0
2018-02-07T22:48:29+0000        ttyUSB0 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2018-02-07T22:48:29+0000        ttyUSB0
2018-02-07T22:49:27+0000        ttyUSB0
2018-02-07T22:49:27+0000        ttyUSB0
2018-02-07T22:49:27+0000        ttyUSB0 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2018-02-07T22:49:27+0000        ttyUSB0
2018-02-07T22:50:11+0000        ttyUSB0
2018-02-07T22:50:11+0000        ttyUSB0
2018-02-07T22:50:11+0000        ttyUSB0 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2018-02-07T22:50:11+0000        ttyUSB0
2018-02-07T22:50:58+0000        ttyUSB0
2018-02-07T22:50:58+0000        ttyUSB0
2018-02-07T22:50:58+0000        ttyUSB0 TcpListener: Accepted connection on socket 16 from address 192.168.0.1.
2018-02-07T22:50:58+0000        ttyUSB0
2018-02-07T22:51:48+0000        ttyUSB0
2018-02-07T22:51:48+0000        ttyUSB0
2018-02-07T22:51:48+0000        ttyUSB0 CryptoTask: Closing connection on socket 16 from address 192.168.0.1.
2018-02-07T22:51:48+0000        ttyUSB0
2018-02-07T23:01:44+0000        ttyUSB0 Audit on 7/2/2018 22:08:36 00200069 0A400000B686296E
2018-02-07T23:01:44+0000        ttyUSB0
2018-02-07T23:02:21+0000        ttyUSB0 Audit on 7/2/2018 22:09:12 00200069 0A4000009D86296E
2018-02-07T23:02:21+0000        ttyUSB0
2018-02-07T23:02:48+0000        ttyUSB0 Audit on 7/2/2018 22:09:39 00200069 0A4000009DC6296E
2018-02-07T23:02:48+0000        ttyUSB0
2018-02-07T23:02:54+0000        ttyUSB0
2018-02-07T23:02:54+0000        ttyUSB0
2018-02-07T23:02:54+0000        ttyUSB0 TcpListener: Closed IPv4 socket 14 on port 5000.
2018-02-07T23:02:54+0000        ttyUSB0
2018-02-07T23:02:54+0000        ttyUSB0
```

```
2018-02-07T23:02:54+0000        ttyUSB0
2018-02-07T23:02:54+0000        ttyUSB0 TcpListener: Closed IPv6 socket 15 on port 5000.
2018-02-07T23:02:54+0000        ttyUSB0
2018-02-07T23:02:54+0000        ttyUSB0 Audit on 7/2/2018 22:09:45 00100003
2018-02-07T23:02:54+0000        ttyUSB0
2018-02-07T23:04:59+0000        ttyUSB0
2018-02-07T23:04:59+0000        ttyUSB0
2018-02-07T23:04:59+0000        ttyUSB0 OP v1 0A400000B7C6296E
2018-02-07T23:04:59+0000        ttyUSB0
2018-02-07T23:05:00+0000        ttyUSB0 Manufacturer: GemPlus
2018-02-07T23:05:00+0000        ttyUSB0
2018-02-07T23:05:00+0000        ttyUSB0 Product: MPCOS EMV
2018-02-07T23:05:00+0000        ttyUSB0
2018-02-07T23:05:01+0000        ttyUSB0 Card Size: 64 kbits
2018-02-07T23:05:01+0000        ttyUSB0
```

Place HSMFDs and OS DVDs into the TEB

Step	Activity	Initials	Time

19.	CA unmounts the HSMFD by executing the following commands on the terminal window
	`cd /tmp`
	`umount /media/HSMFD`
	CA removes the HSMFD, then places it on the holder.
		Y.G.	23:23

20.	CA performs the following steps to switch off the laptop: a) Turn off the laptop by pressing the power switch. b) Turn on the laptop by pressing the power switch and immediately remove the OS DVD from the laptop DVD drive. c) Disconnect all connections to the laptop including power, printer, display and network	Y.G.	23:24
21.	CA places (2) HSMFD, (2) OS DVD, (1) paper with printed HSMFD hash inside the TEB, then seals it.	Y.G.	23:26
22.	CA performs the following steps to verify the TEB: a) Read out the TEB#, then show it to the audit camera above for participants to see. b) Confirm with IW1 that the TEB# match below. c) Initial the TEB with IW1 using a ballpoint pen. d) Give IW1 the sealing strips for later inventory. e) Place the HSM TEB on the cart. OS DVD (release 20170403) + HSMFD: **TEB# BB46592049**	Y.G	23:27

Distribute the HSMFDs

Step	Activity	Initials	Time
23.	CA distributes the remaining HSMFDs: Two for IW1 (for audit bundles). Two for both RKOS (for SKR exchange with RZM and for process review).	Y.G.	23:27

Return the Laptop to TEB

Step	Activity	Initials	Time
24.	CA places the laptop into a prepared TEB, then seals it.	Y.G.	23:28
25.	CA performs the following steps: a) Read out the TEB# and Laptop serial #, then show it to the audit camera above for participants to see. b) Confirm with IW1 that the TEB# and Laptop serial # match below. c) Initial the TEB with IW1 using a ballpoint pen. d) Give IW1 the sealing strips for later inventory. e) Place the Laptop TEB on the cart. Laptop1 (Dell ATG6400): **TEB# BB51184640 / serial # 37240147333**	Y.G.	23:29

Return the OP Cards to TEB

Step	Activity	Initials	Time
26.	One by one, CA calls each COs listed below to the ceremony table to perform the following steps. a) CA takes the OP TEB and plastic case prepared for the CO. b) CO takes his/her OP card from the card holder and places it inside the plastic case. c) CO gives the plastic case containing the OP card to the CA. d) CA places the plastic case into the prepared TEB, reads out the TEB # and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW1 keeps the sealing strips for later inventory. f) IW1 inspects the TEB, confirms the TEB # with the list below, then initials it with a ballpoint pen. g) CA gives the TEB containing the OP card to the CO. h) CO inspects the TEB, verifies its content, then initials it with a ballpoint pen. i) CO writes the date/time and signature on the table of IW1's script, then IW1 initials the entry. j) CO returns to his/her seat with the TEB and careful not to poke or puncture the TEB. k) Repeat steps for all the remaining COs on the list. **CO 1: Arbogast Fabian** OP TEB # **BB46592046** ✓ **CO 2: Dmitry Burkov** OP TEB # **BB46592047** ✓ **CO 3: Joao Damas** OP TEB # **BB46592048** ✓ **CO 4: Carlos Martinez** OP TEB # **BB46592050** ✓ **CO 5: Olafur Gudmundsson** ✓ OP TEB # **BB46592051** **CO 6: Nicolas Antoniello** OP TEB # **BB46592052** ✓ **CO 7: Subramanian Moonesamy** OP TEB # **BB46592053** ✓	YG	23:44

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1 Initials
CO 1	OP 1 of 7	BB46592046	Arbogast Fabian		2018 February 7	23:33 UTC	Y.G.
CO 2	OP 2 of 7	BB46592047	Dmitry Burkov		2018 February 7	23:35 UTC	Y.G.
CO 3	OP 3 of 7	BB46592048	Joao Damas		2018 February 7	23:37 UTC	Y.G.
CO 4	OP 4 of 7	BB46592050	Carlos Martinez		2018 February 7	2339 UTC	Y.G.
CO 5	OP 5 of 7	BB46592051	Olafur Gudmundsson		2018 February 7	23:41 UTC	Y.G.
CO 6	OP 6 of 7	BB46592052	Nicolas Antoniello		2018 February 7	23:42 UTC	Y.G.
CO 7	OP 7 of 7	BB46592053	Subramanian Moonesamy		2018 February 7	23:44 UTC	Y.G.

Return the Equipment to Safe #1

Step	Activity	Initials	Time
27.	CA, IW1, SSC1 enters the safe room with the cart.	Y.G.	23:45
28.	SSC1 opens Safe #1 while shielding the combination from the camera.	Y.G.	23:46
29.	SSC1 removes the safe log and writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	Y.G.	23:47
30.	CA returns each equipment to the Safe by following the steps below: a) CAREFULLY remove the equipment TEB from the cart b) Read out the TEB # while showing it to the audit camera above, then place it inside Safe #1 c) Write the date/time and signature on the safe log where "**Return**" is indicated. d) IW1 verifies the safe log entry, then initials it. HSM4: **TEB# BB51184642 / serial # H1411006** Laptop1: **TEB# BB51184640 / serial # 37240147333** OS DVD (release 20170403) + HSMFD: **TEB# BB46592049**	Y.G.	23:50

Close the Equipment Safe #1

Step	Activity	Initials	Time
31.	SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies this entry, then initials it.	Y.G.	23:50
32.	SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	Y.G.	23:51
33.	CA, SSC1 and IW1 leaves the safe room with the cart, closing the door behind them.	Y.G.	23:51

Open the Credential Safe #2

Step	Activity	Initials	Time
34.	CA and IW1 brings a flashlight, then escorts SSC2, COs with their OP Card and SO Cards (if available) into the safe room.	Y.G	23:52
35.	SSC2 opens Safe #2 while shielding the combination from the camera.	Y.G	23:56
36.	SSC2 removes the safe log and writes the date/time and signature on the safe log where Open Safe is indicated. IW1 verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	Y.G	23:56

CO Returns the Credentials to Safe #2

Step	Activity	Initials	Time
37.	One by one, the selected CO returns the TEBs of OP card by following the steps below. a) CO reads out their OP card TEB#, then verifies its integrity while showing it to the audit camera above b) With the assistance of the CA (and his/her common key), the CO opens his/her safe deposit box. **Note: Common Key is for the bottom lock. CO Key is for the top lock** c) CO reads out the safe deposit box number, places his/her TEBs inside it, then locks it. d) CO writes the date/time and signature on the safe log "Return OP Card" is indicated. e) IW1 verifies the completed safe log entry, then initials it. Repeat these steps until all the required cards listed below are returned. **CO 1: Arbogast Fabian - Box # 1791** ✓ **OP TEB # BB46592046** **CO 2: Dmitry Burkov - Box # 1793** ✓ **OP TEB # BB46592047** **CO 3: Joao Damas - Box # 1071** ✓ **OP TEB # BB46592048** **CO 4: Carlos Martinez - Box # 1068** ✓ **OP TEB # BB46592050** **CO 5: Olafur Gudmundsson - Box # 1789** ✓ **OP TEB # BB46592051** **CO 6: Nicolas Antoniello - Box # 1073** **OP TEB # BB46592052** ✓ **CO 7: Subramanian Moonesamy - Box # 1792** **OP TEB # BB46592053** ✓	Y.S	00:05

Close the Credential Safe #2

Step	Activity	Initials	Time
38.	Once all relevant deposit boxes are closed and locked, SSC2 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies the safe log entry, then initials it.	Y.G.	00:05
39.	SSC2 returns the safe log back to Safe #2, then locks it (spin dial must go at least two full revolutions each way, counter clock-wise then clock-wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	Y.G.	00:06
40.	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	Y.G.	00:08

Act 5. Close the Key Signing Ceremony

Participants Signing of IW1's Script

Step	Activity	Initials	Time
1.	CA reads the exceptions that may have occurred during the ceremony.	Y.G.	00:07
2.	CA calls each attendee on the participants list to proceed to the ceremony table and **sign IW1's participants list. All signatures declare that this script is a true and accurate record of the ceremony.** IW1 records the completion time once all participants have signed the list.	Y.G.	00:11
3.	CA reviews IW1's script and signs on the participants list.	Y.G	00:13
4.	CA acknowledges everyone's participation and notifies them that the Root DNSSEC KSK Signing Ceremony 32 has been completed. **Note: On-site participants that will not attend the HSM Destruction ceremony must sign out of the ceremony room log and will be escorted out of the facility.**	Y.G.	00:15

Bundle Audit Materials

Step	Activity	Initials	Time
	IW1 makes (1) copy of his/her script for off-site audit bundle. Each Audit bundle contains: a) Output of signer system – HSMFD b) Copy of IW1's key ceremony script c) Audio-visual recording d) Logs from the Physical Access Control System and Intrusion Detection System (Range is **2017/08/17 – 2018/02/08)** e) IW1 attestation (Section A.1) f) SA1 attestation (Sections A.2 and A.3) All TEBs are labeled **"Root DNSSEC KSK Ceremony 32"**, dated and signed by **IW1 and CA**. Audit bundles are delivered to an off-site storage. **Note:** The CA holds the ultimate responsibility to finalize the audit bundle collection	Y.G.	02:55

Audit Bundle Checklist:

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

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

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

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

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

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

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

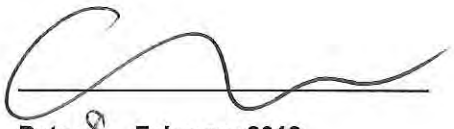
6. Configuration review of the Firewall System (SA1)
SA1's attestation and hard copies of the firewall configuration from the review process. See Appendix A.3. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Other items
If applicable.

A.1 Key Ceremony Script (by IW1)

I hereby attest that the Key Ceremony was conducted in accordance to this script.
Any exceptions that may have occurred, were accurately and properly documented.

Yuko Green



Date: 8 February 2018

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

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

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

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

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

Connor Barthold

Date: 08 February 2018

A.3 Firewall Configuration Review (by SA1)

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

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

Connor Barthold

Date: 08 February 2018

```
cbarthold@srx# run show configuration | no-more
## Last commit: 2017-01-12 22:30:47 UTC by jjenkins
version 12.1X46-D35.1;
system {
    host-name srx;
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
    }
    name-server {
        8.8.8.8;
        8.8.4.4;
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh {
            root-login deny;
        }
        netconf {
            ssh;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
chassis {
    config-button no-rescue no-clear;
}
interfaces {
    interface-range access {
        member-range ge-0/0/0 to ge-0/0/8;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-access;
                }
            }
        }
    }
    interface-range video {
        member-range ge-0/0/9 to ge-0/0/12;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-video;
                }
            }
        }
    }
    interface-range wifi {
        member ge-0/0/13;
        unit 0 {
            family inet {
                address 10.100.1.1/24;
            }
        }
    }
    interface-range guest {
        member ge-0/0/14;
        member ge-0/0/15;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-guest;
                }
            }
        }
    }
    ge-0/0/0 {
        description "Access Control Server";
    }
    ge-0/0/1 {
        description "Access Control Client Custom Solution";
    }
    ge-0/0/2 {
        description "Intrusion Detection Panel";
    }
    ge-0/0/3 {
        description "Environment Monitoring";
    }
    ge-0/0/4 {
        description "Monitoring Server";
    }
    ge-0/0/5 {
        description "IRIS Enrollment";
    }
    ge-0/0/6 {
        description "Iris Scanner T2";
        /* Not available at KMF-West */
        disable;
    }
    ge-0/0/7 {
        description "Iris Scanner T3";
    }
    ge-0/0/8 {
        description "Iris Scanner T4";
    }
    ge-0/0/9 {
        description "Video Surveillance Server";
    }
    ge-0/0/10 {
        description "Camera 1";
    }
    ge-0/0/11 {
        description "Camera 2";
    }
    ge-0/0/12 {
        description "Camera 3";
    }
    ge-0/0/13 {
        description "Wifi Connection";
    }
    ge-0/0/14 {
        description "Streaming Laptop";
    }
    ge-0/0/15 {
        description "Audio Camera Client";
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 192.0.35.202/26;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input route-engine-filter;
                }
            }
        }
    }
    st0 {
        unit 1 {
            description "IPSec KMF-West";
            family inet;
        }
    }
    vlan {
        unit 0 {
```

```
        family inet {
            address 10.4.28.193/26;
        }
    }
    unit 1 {
        family inet {
            address 10.4.28.129/26;
        }
    }
    unit 2 {
        family inet {
            address 10.4.28.1/25;
        }
    }
  }
}
routing-options {
  static {
    route 0.0.0.0/0 next-hop 192.0.35.201;
    route 10.4.29.0/24 next-hop st0.1;
    route 152.194.1.148/32 next-hop 192.0.35.201;
  }
}
policy-options {
  prefix-list resolver-servers {
    8.8.4.4/32;
    8.8.8.8/32;
  }
  prefix-list local-prefixes {
    10.4.28.0/24;
  }
  prefix-list ntp-servers {
    129.6.15.28/32;
    129.6.15.29/32;
  }
}
security {
  ike {
    policy ike-policy-KMF {
      pre-shared-key ascii-text "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
    }
    gateway Gateway-to-KMF-East {
      ike-policy ike-policy-KMF;
      address 152.194.1.148;
      external-interface ge-1/0/0;
    }
  }
  ipsec {
    traceoptions {
      flag all;
    }
    proposal IPSecProposal {
      protocol esp;
      authentication-algorithm hmac-sha-256-128;
      encryption-algorithm aes-256-cbc;
      lifetime-seconds 7200;
    }
    policy defaultPolicy {
      perfect-forward-secrecy {
        keys group5;
      }
      proposals IPSecProposal;
    }
    vpn vpn-to-KMF-East {
      bind-interface st0.1;
      ike {
        gateway Gateway-to-KMF-East;
        ipsec-policy defaultPolicy;
      }
      establish-tunnels immediately;
    }
  }
  screen {
    ids-option external-screen {
      icmp {
        ping-death;
      }
      ip {
        source-route-option;
        tear-drop;
      }
      tcp {
        syn-flood {
          alarm-threshold 1024;
          attack-threshold 200;
          source-threshold 1024;
          destination-threshold 2048;
          timeout 20;
        }
        land;
      }
    }
  }
  nat {
    source {
      rule-set internal-to-external {
        from zone [ access guest wifi ];
        to zone untrust;
        rule source-nat-rule {
          match {
            source-address 0.0.0.0/0;
          }
          then {
            source-nat {
              interface;
            }
          }
        }
      }
    }
  }
}
policies {
  from-zone access to-zone untrust {
    policy allow-mail {
      match {
        source-address [ ACC ACS EVM IMS ];
        destination-address icann;
        application junos-smtp;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
    policy allow-dns {
      match {
        source-address [ ACC ACS EVM IMS ];
        destination-address [ icann-dns google-dns ];
        application [ junos-dns-udp junos-dns-tcp ];
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
    policy allow-simplex {
      match {
        source-address IDP;
        destination-address simplex;
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
  from-zone access to-zone video {
    policy access-to-video {
      match {
        source-address IMS;
        destination-address kmf_west_video;
        application junos-icmp-all;
      }
      then {
        permit;
      }
    }
  }
  from-zone access to-zone ipsec {
    policy allow-access-to-ipsec {
      match {
        source-address [ ACS ACC ];
        destination-address [ kmf_east_acs kmf_east_acc ];
        application any;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
    policy allow-icmp {
      match {
        source-address any;
        destination-address any;
        application junos-icmp-ping;
      }
      then {
        permit;
      }
    }
    policy allow-access-access {
      match {
        source-address kmf_west_access;
        destination-address kmf_east_access;
        application any;
      }
      then {
        permit;
      }
    }
  }
  from-zone ipsec to-zone access {
    policy allow-ipsec-to-access {
      match {
        source-address [ kmf_east_acs kmf_east_acc ];
        destination-address [ ACS ACC ];
        application any;
      }
      then {
        permit;
        log {
```

```
            session-close;
          }
        }
      }
      policy allow-icmp {
        match {
          source-address any;
          destination-address any;
          application junos-icmp-ping;
        }
        then {
          permit;
        }
      }
      policy allow-access-access {
        match {
          source-address kmf_east_access;
          destination-address kmf_west_access;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone video to-zone ipsec {
      policy allow-video-to-ipsec {
        match {
          source-address VSS;
          destination-address kmf_east_vss;
          application any;
        }
        then {
          permit;
          log {
            session-close;
          }
        }
      }
      policy allow-access-video {
        match {
          source-address kmf_west_video;
          destination-address kmf_east_video;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone guest to-zone untrust {
      policy allow-guest-to-untrust {
        match {
          source-address kmf_west_guest;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone wifi to-zone untrust {
      policy allow-wifi-to-untrust {
        match {
          source-address kmf_west_wifi;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone ipsec to-zone video {
      policy allow-ipsec-to-video {
        match {
          source-address kmf_east_vss;
          destination-address VSS;
          application any;
        }
        then {
          permit;
          log {
            session-close;
          }
        }
      }
      policy allow-icmp {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
      policy allow-access-video {
        match {
          source-address kmf_east_video;
          destination-address kmf_west_video;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone access to-zone access {
      policy allow-access {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone video to-zone video {
      policy allow-ntp {
        match {
          source-address any;
          destination-address video-ntp-server;
          application junos-ntp;
        }
        then {
          permit;
        }
      }
    }
    default-policy {
      deny-all;
    }
  }
  zones {
    security-zone access {
      address-book {
        address ACS 10.4.28.203/32;
        address ACC 10.4.28.202/32;
        address IDP 10.4.28.201/32;
        address EVM 10.4.28.200/32;
        address IMS 10.4.28.204/32;
        address E1 10.4.28.210/32;
        address E3 10.4.28.212/32;
        address E4 10.4.28.213/32;
        address kmf_west_access 10.4.28.192/26;
        address localnet 10.4.28.0/24;
        address-set iris-scanners {
          address E1;
          address E3;
          address E4;
        }
      }
      interfaces {
        vlan.0 {
          host-inbound-traffic {
            system-services {
              ping;
              ntp;
            }
          }
        }
      }
    }
    security-zone untrust {
      address-book {
        address icann 192.0.32.0/20;
        address icann-dns 192.0.42.53/32;
        address googledns1 8.8.8.8/32;
        address googledns2 8.8.4.4/32;
        address simplex1 216.224.218.31/32;
        address simplex2 216.224.218.32/32;
        address simplex3 216.224.218.33/32;
        address simplex4 216.224.218.34/32;
        address-set google-dns {
          address googledns1;
          address googledns2;
        }
        address-set simplex {
          address simplex1;
          address simplex2;
          address simplex3;
          address simplex4;
        }
      }
      screen external-screen;
      interfaces {
        ge-1/0/0.0 {
          host-inbound-traffic {
            system-services {
              ping;
              ssh;
            }
          }
        }
      }
    }
    security-zone video {
      address-book {
        address kmf_west_video 10.4.28.128/26;
        address VSS 10.4.28.150/32;
        address C1 10.4.28.151/32;
        address C2 10.4.28.152/32;
        address C3 10.4.28.153/32;
        address video-ntp-server 10.28.4.129/32;
        address-set cameras {
          address C1;
```

```
            address C2;
            address C3;
          }
        }
        interfaces {
          vlan.1 {
            host-inbound-traffic {
              system-services {
                ping;
              }
            }
          }
        }
      }
      security-zone guest {
        address-book {
          address STR 10.4.28.20/32;
          address VCC 10.4.28.22/32;
          address kmf_west_guest 10.4.28.0/25;
        }
        interfaces {
          vlan.2 {
            host-inbound-traffic {
              system-services {
                ping;
              }
            }
          }
        }
      }
      security-zone ipsec {
        address-book {
          address kmf_east_access 10.4.29.192/26;
          address kmf_east_video 10.4.29.128/26;
          address kmf_east_acs 10.4.29.204/32;
          address kmf_east_acc 10.4.29.202/32;
          address kmf_east_idp 10.4.29.201/32;
          address kmf_east_evm 10.4.29.200/32;
          address kmf_east_ims 10.4.29.203/32;
          address kmf_east_E1 10.4.29.210/32;
          address kmf_east_E2 10.4.29.211/32;
          address kmf_east_E3 10.4.29.212/32;
          address kmf_east_E4 10.4.29.213/32;
          address kmf_east_vss 10.4.29.150/32;
          address kmf_east_C1 10.4.29.151/32;
          address kmf_east_C2 10.4.29.152/32;
          address kmf_east_C3 10.4.29.153/32;
        }
        interfaces {
          st0.1 {
            host-inbound-traffic {
              system-services {
                ping;
                ike;
                ssh;
              }
            }
          }
        }
      }
      security-zone wifi {
        address-book {
          address kmf_west_wifi 10.100.1.0/24;
        }
        interfaces {
          ge-0/0/13.0 {
            host-inbound-traffic {
              system-services {
                ping;
              }
            }
          }
        }
      }
    }
  }
}
firewall {
  family inet {
    filter route-engine-filter {
      term deny-icmp-redirects {
        from {
          protocol icmp;
          icmp-type redirect;
        }
        then {
          discard;
        }
      }
      term allow-icmp {
        from {
          protocol icmp;
          icmp-type [ echo-request echo-reply unreachable time-exceeded ];
        }
        then {
          policer small-bw-limit;
          accept;
        }
      }
      term allow-traceroute {
        from {
          protocol udp;
          port 33434-33534;
        }
        then {
          policer small-bw-limit;
          accept;
        }
      }
      term allow-dns {
        from {
          source-prefix-list {
            resolver-servers;
          }
          protocol udp;
          source-port domain;
        }
        then {
          policer small-bw-limit;
          accept;
        }
      }
      term allow-ntp {
        from {
          source-prefix-list {
            local-prefixes;
            ntp-servers;
          }
          protocol udp;
          port ntp;
        }
        then {
          policer small-bw-limit;
          accept;
        }
      }
      term allow-establish {
        from {
          protocol tcp;
          tcp-established;
        }
        then accept;
      }
      term allow-ipsec-esp {
        from {
          protocol esp;
        }
        then accept;
      }
      term allow-ipsec-udp {
        from {
          protocol udp;
          port 500;
        }
        then accept;
      }
      term allow-ssh {
        from {
          source-address {
            152.194.1.148/32;
            10.4.29.0/24;
            10.4.28.0/24;
          }
          protocol tcp;
          destination-port ssh;
        }
        then accept;
      }
      term LAST {
        then {
          discard;
        }
      }
    }
    policer small-bw-limit {
      if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
      }
      then discard;
    }
  }
  poe {
    interface all;
  }
  vlans {
    vlan-access {
      vlan-id 3;
      l3-interface vlan.0;
    }
    vlan-guest {
      vlan-id 5;
      l3-interface vlan.2;
    }
    vlan-video {
      vlan-id 4;
      l3-interface vlan.1;
    }
  }
```