Root DNSSEC KSK Ceremony 34

Wednesday August 15, 2018

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

This ceremony is executed in accordance to 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 described on https://www.iana.org/help/key-ceremony-roles
Instructions: At the end of the ceremony, participants sign IW's script. IW records time of completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Gustavo Lozano / ICANN		2018 Aug 15	2344
IW	Patrick Jones / ICANN			
SSC1	Anand Mishra / ICANN			
SSC2	Jessica Castillo / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Ryan Brown / Verisign			
RZM	Trevor Davis / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Catherine Choy / RSM			
AUD	Micah Springer / RSM			
SA	Connor Barthold / ICANN			
SA	Mike Brennan / ICANN			
RKOS / CA Backup	Alberto Duero / PTI	FUNKY		
RKOS / IW Backup	Andres Pavez / PTI			
SW	Leticia Castillo / ICANN			
SW	Joseph Restuccia / ICANN			
SW	Laura Bengford / ICANN			
~~SW~~	~~Paula Wang / PTI~~			
SW	David Prangnell / PTI			
SW	Kim Davies / PTI			

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. Only CAs, IWs or SAs can enter and escort other participants into the Ceremony room. Dual Occupancy is enforced. IW with CA or SA must remain inside the Ceremony room if participants are present in the room. CAs, IWs or SAs may escort participants out of the Ceremony room at the CA's discretion only if the Safe room is not occupied during ceremony. 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.	PJ	20:02
2	CA confirms that all participants are signed into the Ceremony Room, then performs a roll call using the list of participants on page 2.	PJ	20:07

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3	CA reviews the emergency evacuation procedure with onsite participants.	PJ	20:07
4	CA explains the use of personal electronic devices during ceremony.	PJ	20:08
5	CA briefly explains the purpose of the ceremony.	PJ	20:09

Verify the Time and Date

Step	Activity	Initials	Time
6	IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 20.10.13 All entries into this script or any logs should follow this common source of time.	PJ	20:10

Open the Credential Safe #2

Step	Activity	Initials	Time
7	CA and IW brings a flashlight and escorts the SSC2 and the COs into the safe room.	PJ	20:11
8	SSC2 opens Safe #2 while shielding the combination from the camera.	PJ	20:13
9	Perform the following steps to complete the safe log: a) SSC2 takes out the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date, time and signature on the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.	PJ	20:15

COs Extract the Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10	One by one, the selected CO performs the following steps to retrieve the required TEBs: a) With the assistance of the CA (and the 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.** b) CO reads out the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB. c) CO reads out the TEB numbers, then verifies its integrity while showing it to the audit camera above. d) CO retains the TEB specified below, then locks the safe deposit box. e) CO writes the date, time and signature on the safe log where removal of TEBs are indicated. f) IW verifies the completed safe log entries, then initials it. **CO1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46592046 (Retain)** ✓ **SO TEB # BB46584451 (Check and Return)** ✓ **CO2: Dmitry Burkov** **Box # 1793** **OP TEB # BB46592047 (Retain)** ✓ **SO TEB # BB46584453 (Check and Return)** ✓ **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46592052 (Retain)** ✓ **SO TEB # BB46584459 (Check and Return)** ✓ **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46592053 (Retain)** ✓ **SO TEB # BB46584461 (Check and Return)** ✓	PJ PJ PJ PJ	20:17 20:19 20:20 20:22

Close the Credential Safe #2

Step	Activity	Initials	Time
11	Once all deposit boxes are closed and locked, SSC2 writes the date, time and signature on the safe log where "Close Safe" is indicated. IW verifies the entry then initials it.	PJ	20:22
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 IW verifies that the safe is locked and the "WAIT" light indicator is off.	PJ	20:23
13	CA, IW, SSC2, and COs leave the safe room with TEBs, closing the door behind them.	PJ	2024

Open Equipment Safe #1

Step	Activity	Initials	Time
14	CA and IW brings a cart and escorts the SSC1 into the safe room.	[illegible]	2025
15	SSC1 opens Safe #1 while shielding the combination from the camera.	PD	2027
16	Perform the following steps to complete the safe log: a) SSC1 takes out the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date, time and signature on the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.	PD	2027

Remove the Equipment from Safe #1

Step	Activity	Initials	Time
17	CA performs the following steps to extract each equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read out each TEB number, then verify its integrity while showing it to the audit camera. c) Place each 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) IW verifies the safe log entry, then initials it. **HSM3: TEB # BB51184623 / Serial # H1403033 (Place on cart)** **HSM4: TEB # BB51184642 / Serial # H1411006 (Check and Return)** **Laptop1: TEB # BB51184640 / Serial # 37240147333 (Place on cart)** **Laptop2: TEB # BB24646591 / Serial # 7292928457 (Check and Return)** **Laptop3: TEB # BB81420139 / Service Tag # C8SVSG2 (Place on cart)** **Laptop4: TEB # BB81420138 / Service Tag # F8SVSG2 (Check and Return)** **OS DVD (release 20170403) + HSMFD: TEB # BB46592049 (Place on cart)** **Note: The Service Tag # is the same as the Serial Number.**	PD	2034

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. IW verifies the safe log entry then initials it.	PD	2035
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 IW verifies that the safe is locked and the "WAIT" light indicator is off.	PD	20:36
20	CA, IW and SSC1 leaves the safe room with the cart, closing the door behind them.	PD	2037

Act 2. OS DVD Acceptance Test

Setup Equipment

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the listed equipment: a) Remove the equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read out the TEB number and the serial number (if applicable) while IW matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place the equipment on its designated area on the ceremony table. **Laptop1: TEB # BB51184640 / Serial # 37240147333** **OS DVD (release 20170403) + HSMFD: TEB # BB46592049**	PJ	20:40
2	CA performs the following steps to boot the laptop: a) Connect the USB of the general purpose external DVD drive. b) Connect the external display, then the power supply. c) Immediately insert the **OS DVD release 20170403** into the laptop DVD try after the laptop power is switched ON.	PJ	20:42
3	CA performs the following steps to setup the laptop: 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 the external display works. e) Log in as `root`	PJ	20:47
4	CA opens a terminal window through: **Applications > Accessories > Terminal** CA performs the following steps to increase its visibility: a) Click the **View** menu and select **Zoom In.** b) Repeat the step above as necessary.	PJ	20:48

OS DVD Acceptance Test

Step	Activity	Initials	Time

5	CA inserts the new **OS DVD release coen-0.4.0** into the external DVD drive, waits for it to be recognized by the OS, then performs the following steps:
	a) Close the file system popup window.
	CA uses the terminal window to continues with the following steps:
	b) Confirm the drive letter by executing:
	`df`
	c) Unmount the drive by executing:
	`umount /dev/scd1`
	d) Calculate the SHA-256 hash by executing:
	`sha2wordlist < /dev/scd1`
	
	IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.
	
	SHA-256 hash:
	8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f
	
	PGP Words:
	minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document
	
	Note: The SHA-256 hash of the OS DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/34
		PJ	20:50
			2052

6	CA removes the OS DVD by pressing the eject button on the external DVD drive, then places it on the ceremony table. **Note: The tested OS DVD must be placed on the ceremony table where it is visible to the audit camera and the participants**	PJ	2052
7	CA repeats step 5 to 6 for the 2nd copy of the new **OS DVD release coen-0.4.0.**	PJ	2055
8	IW records his/her signature upon successful completion of the **OS DVD release coen-0.4.0** acceptance testing. Printed Name: **Patrick Jones** Signature: Patrick Jones Date: **2018/08/15**	PJ	2055

Return the OS DVDs and Laptop to TEB

Step	Activity	Initials	Time
9	CA performs the following steps to switch OFF the laptop and remove the OS DVD: a) Turn OFF the laptop by pressing the power switch button. b) Turn ON the laptop and immediately remove the OS DVD from it. c) Disconnect all connections from the laptop including power, display and external DVD drive.	PS	2056
10	CA performs the following steps to return the equipment to TEB: a) CA places 2 **OS DVD release 20170403** into a prepared TEB, then seals it. b) CA places the Laptop1 into a prepared TEB, then seals it.	PS	2059
11	CA performs the following steps to verify the TEBs: a) Read out the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches with the information below. c) Initial the TEB with IW using a ballpoint pen. d) Give IW the sealing strips for later inventory. e) Place the TEB on the cart. **OS DVD release 20170403: TEB # BB46592068** ✓ **Laptop1: TEB # BB51184666 / Serial # 37240147333** ✓	PS	2100

Act 3. Setup Equipment

Setup Laptop

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the listed equipment: a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read out the TEB number and the serial number (if applicable) while IW matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place the equipment on its designated area on the ceremony table. **HSM3: TEB # BB51184623 / Serial # H1403033** **Laptop3: TEB # BB81420139 / Serial # C8SVSG2**	PJ	2103
2	CA performs the following steps to boot the laptop: a) Connect the USB printer cable into the back USB slot of the laptop. b) Connect the Null Modem cable into the Serial Port of the laptop. c) Connect the external HDMI display. d) Connect the power supply. e) Immediately insert the **OS DVD release coen-0.4.0** after the laptop power is switched ON.	PJ	2105
3	CA verifies if the external display works, then perform adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	PJ	2107

PJ 2157

Setup Printer

Step	Activity	Initials	Time
4	CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page: `configure-printer`	PJ	2108

PJ 2157

Setup Date

Step	Activity	Initials	Time
5	CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock. If the date/time do not match, perform the following steps: a) Execute `date -s "20180815 HH:MM:00"` to set the time. **where `HH` is two-digit hour, `MM` is two-digit minutes and `00` is zero seconds.** b) Execute `date` to confirm the date/time matches the clock.	PJ	2108

PJ 2157

Format and label the blank FD

Step	Activity	Initials	Time

6	CA performs the following steps to format a new FD:
	a) Plug a new FD into the USB slot of the laptop and wait for it to be recognized.
	b) Close the file system popup window.
	CA uses the terminal window to continue with the following steps:
	c) Confirm the drive letter by executing:
	`df`
	d) Unmount the drive by executing:
	`umount /dev/sdb1`
	e) Format and label the FD by executing:
	`mkfs.vfat -n HSMFD -I /dev/sdb1`
	f) CA removes the FD, then places it on the holder.
		PS	21:11

7	CA repeats step 6 for the 2nd blank FD.	PS	21:12
8	CA repeats step 6 for the 3rd blank FD.	PS	21:13
9	CA repeats step 6 for the 4th blank FD.	PS	21:13
10	CA repeats step 6 for the 5th blank FD.	PS	21:14

Connect the HSMFD

Step	Activity	Initials	Time
11	CA plugs the **Ceremony 32 HSMFD** into the USB slot, then performs the following steps: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window. d) Give the unused **HSMFD 32** to IW.	PS	21:16
12	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash -c` IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 32 annotated script. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.** SHA-256: e3d877c855ec3d1a1f97f07c397e7b75c208f0afa7ef65811b45396d5bb246fe PGP Words: tissue stupendous involve retrieval edict unicorn commence Bradbury billiard mosquito unearth informant classroom insurgent kickoff impartial snapshot antenna unearth pharmacy repay unravel fracture inventive beeswax detector classroom hazardous erase pioneer cubic yesteryear	PS	21:20

PS 2159

Exception 1

Root DNSSEC Script Exception #1

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 3 Step(s): 12 Page(s): 12 Date and Time: 2018|08|15	PJ	21:27
2.	IW describes the exception(s) and action(s) below.	PJ	21:27

The hash from the previous ceremony was different from what was on the script. We will try to generate the hash using the previous operating system. We opened the old OS DVD TEB. The new TEP numbers for OS DVD v. 20170403 are: BB46592073
We continued with Step 11, Act 3 with the old OS DVD. The new laptop did not recognize the HSM FD, so we had to use the old laptop.
The new TEB for LAPTOP 1 is: BB51184691. SN 37240147333
We repeated Step 3 from Act #2, returned to Step 12 from Act 3
The hash was a match to hash from ceremony 32. We continued the ceremony with the new laptop. Before moving ahead, we repeated the steps using the other HSMFD. The hash was the same as ceremony 32.
We continued the ceremony with the new OS and the new laptop.

Start the Terminal Session Logging

Step	Activity	Initials	Time
13	CA executes the command below using the terminal window to change the detault directory to HSMFD: `cd /media/HSMFD`	PS	2159
14	CA executes the command below to log activities of the **Commands** terminal window : `script script-20180815.log`	PS	2200

Start the HSM Activity Logging

Step	Activity	Initials	Time

15	CA performs the following steps using the **HSM Output** terminal window to capture the activity logs of the HSM:
	a) Change the default directory to HSMFD by executing:
	`cd /media/HSMFD`
	b) Set the serial port baud rate by executing:
	`stty -F /dev/ttyS0 115200`
	c) Start logging the serial output by executing:
	`ttyaudit /dev/ttyS0`
	Note: DO NOT unplug the serial null modem cable from the laptop as this will stop capturing activity logs from the serial port.
		PS	2202

Power ON the HSM

Step	Activity	Initials	Time
16	CA performs the following steps to prepare the HSM: a) Plug the serial null modem serial cable to the HSM. b) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** c) Scroll the logging screen up and look for the HSM serial number. d) IW matches the displayed HSM serial number on the screen with the information below. **HSM3: Serial # H1403033** ✓ **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	PS	22.04

Act 4. Activate HSM and Generate Signatures

Enable/Activate the HSM

Step	Activity	Initials	Time
1	One by one, CA calls each COs listed below to perform the following steps: a) CO reads out the TEB number, then CA inspects it for tamper evidence. b) CO opens the TEB, then gives the plastic case and card to the CA. c) CA keeps the plastic case, then places the card on the card holder that is visible to everyone. **CO1: Arbogast Fabian** **OP TEB # BB46592046** ✓ **CO2: Dmitry Burkov** **OP TEB # BB46592047** ✓ **CO6: Nicolas Antoniello** **OP TEB # BB46592052** ✓ **CO7: Subramanian Moonesamy** **OP TEB # BB46592053** ✓	PB PD PO PB	22:05 22:07 22:08 22:08
2	CA performs the following steps to activate the **HSM**: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, hit **ENT** to confirm. c) When **"Set Online?"** is displayed, hit **ENT** to confirm. d) When **"Insert Card OP #?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW 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 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PB	22:11

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
3	CA connects the HSM to the laptop using Ethernet cable in LAN port.	PS	2211

4	CA performs the following steps to test the network connectivity between laptop and HSM:
	a) Use the **Commands** terminal window
	b) Test connectivity by executing:
	`ping hsm`
	c) Wait for responses, then exit by pressing:
	`Ctrl + C`
		PS	22:12

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 4 KSRs. 1 for normal operation and the rest for fallback scenario(s).**	PS	22:14

Execute the KSR Signer for Phase D to E

Step	Activity	Initials	Time
6	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK34-0-D_to_E/ksr-root-2018-q4-0-d_to_e.xml`	PS	22:15
7	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	PS	2215

Verify the KSR Hash for Phase D to E

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed on the terminal window, 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 IW to review. b) RZM representative reads out the PGP word list SHA-256 hash of the KSR file being used. c) IW retains the documents provided by the RZM representative and writes the name : RYAN BROWN	PS	2217
9	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	PS	2217
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/KSK34-0-D_to_E/skr-root-2018-q4-0-d_to_e.xml`	PS	2218

Execute the KSR Signer for Phase E to D

Step	Activity	Initials	Time
11	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK34-1-E_to_D/ksr-root-2018-q4-1-e_to_d.xml`	PS	2219
12	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	PS	2219

Verify the KSR Hash for Phase E to D

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.	PS	22:20
14	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	PS	22:20
15	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located on: `/media/KSR/KSK34-1-E_to_D/skr-root-2018-q4-1-e_to_d.xml`	PS	22:20

VERISIGN™

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

Verisign.com

August 15th, 2018

To Whom It May Concern:

This is a letter of Verification of Employment for Ryan Brown. Verisign, Inc. has employed Ryan Brown full-time since April 18th, 2016, currently as a Sr. Manager - Provisioning Ops Sys Admin in our Production 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

VERISIGN

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

verisign.com

15 August 2018

The SHA256 hash of the 2018 Q4 KSR file is:

ksr-root-2018-q4-0-d_to_e.xml:

945278a94defdcb4c78524a91bdd80575841680c6ae1fe08fbe6beed0cb068cf

The PGP wordlist for the hash above is:

Pluto enrollment island passenger dreadful unravel sweatband politeness soybean leprosy bluebird passenger beeswax tambourine merit Eskimo endorse decadence frighten article Geiger tolerance woodlark antenna watchword trombonist skydive unify ammo phonetic frighten Saturday

Attested on behalf of VeriSign by:

Ryan Brown
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

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

verisign.com

15 August 2018

The SHA256 hash of the 2018 Q4 KSR file is:

ksr-root-2018-q4-1-e_to_d.xml:

494e5c10fd124e85fdb25e94e6ca6abbe87f3f6b23417554ca94 6e830b76647f

The PGP wordlist for the hash above is:

deckhand distortion escape autopsy willow backwater drifter leprosy willow pioneer eyeglass molecule tracker revenue Geiger publisher trauma integrate cowbell Hamilton blowtorch decadence indulge equation spellbind molecule goldfish Jamaica alone impetus flytrap integrate

Attested on behalf of VeriSign by:

Ryan Brown
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

VERISIGN

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

verisign.com

15 August 2018

The SHA256 hash of the 2018 Q4 KSR file is:

ksr-root-2018-q4-2-d_to_d.xml:

eaba26f2c0238eb74e14cd7a33f29d1de0a1210cc442c0dddcdb dccea96b4a4b

The PGP wordlist for the hash above is:

Trojan puberty bookshelf vagabond slowdown cannonball orca processor drifter belowground spindle infancy chisel vagabond quadrant breakaway tapeworm outfielder blackjack article snowslide December slowdown tambourine sweatband suspicious sweatband sardonic revenge Hamilton dogsled disable

Attested on behalf of VeriSign by:

Ryan Brown
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

VERISIGN

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

verisign.com

15 August 2018

The SHA256 hash of the 2018 Q4 KSR file is:

ksr-root-2018-q4-3-c_to_c.xml:

7f3ebe5d20bf96c8f79210e246e660a8a59e0edf2fb27202d902ecbd288a4155

The PGP wordlist for the hash above is:

lockup cumbersome skydive filament bison rebellion prefer retrieval virus misnomer assume tomorrow cubic trombonist facial paramount reindeer onlooker apple therapist cement pioneer highchair aftermath sugar aftermath tumor quantity breadline maverick cranky equipment

Attested on behalf of VeriSign by:

Ryan Brown
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

Execute the KSR Signer for Phase D to D

Step	Activity	Initials	Time
16	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK34-2-D_to_D/ksr-root-2018-q4-2-d_to_d.xml`	PS	22:20
17	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	PS	22:21

Verify the KSR Hash for Phase D to D

Step	Activity	Initials	Time
18	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.	PS	22:21
19	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	PS	22:22
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/KSK34-2-D_to_D/skr-root-2018-q4-2-d_to_d.xml`	PS	22:22

Execute the KSR Signer for Phase C to C

Step	Activity	Initials	Time
21	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK34-3-C_to_C/ksr-root-2018-q4-3-c_to_c.xml`	PS	22:22
22	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	PS	22:22

Verify the KSR Hash for Phase C to C

Step	Activity	Initials	Time
23	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.	PS	22:22
24	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	PS	22:23
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/KSK34-3-C_to_C/skr-root-2018-q4-3-c_to_c.xml`	PS	22:23

```
Starting: ksrsigner /media/KSR/KSK34-0-D_to_E/ksr-root-2018-q4-0-d_to_e.xml (at Wed Aug 15 22:15:23 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.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-0-D_to_E/ksr-root-2018-q4-0-d_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
945278A94DEFDCB4C78524A91BDD80575841680C6AE1FE08FBE6BEED0CB068CF
>> Pluto enrollment island passenger dreadful unravel sweatband politeness soybean leprosy bluebird passenger beeswax tam
bourine merit Eskimo endorse decadence frighten article Geiger tolerance woodlark antenna watchword trombonist skydive un
ify ammo phonetic frighten Saturday <<

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/KSK34-0-D_to_E/skr-root-2018-q4-0-d_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749   20326(Klajeyz)/S,19036(Kjqmt7v)/P

SHA256 hash of SKR:
758A33F0E57D53999B48B65F4DFB77F3F3311A19D1A18CB4386BEA611DDB32CE
>> indulge maverick chisel upcoming topmost insincere dwelling nebula puppy dictator Scotland forever dreadful Wichita in
volve vertigo upset company beehive bottomless stairway outfielder offload politeness classic Hamilton Trojan frequency B
elfast suspicious checkup sardonic <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK34-1-E_to_D/ksr-root-2018-q4-1-e_to_d.xml (at Wed Aug 15 22:18:58 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.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:          ICANNKSK
    ManufacturerID: Ultra Electronics AEP Networks
    Model:          Keyper 9860-2
    Serial:         H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-1-E_to_D/ksr-root-2018-q4-1-e_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
494E5C10FD124E85FDB25E94E6CA6ABBE87F3F6B23417554CA946E830B76647F
>> deckhand distortion escape autopsy willow backwater drifter leprosy willow pioneer eyeglass molecule tracker revenue G
eiger publisher trauma integrate cowbell Hamilton blowtorch decadence indulge equation spellbind molecule goldfish Jamaic
a alone impetus flytrap integrate <<

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/KSK34-1-E_to_D/skr-root-2018-q4-1-e_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
A7B38B0963C9371BAAD0B9239107EE77927CCFAE59CD91AB8D6D73DC910F742A
>> repay pocketful obtuse applicant flatfoot retrospect clamshell bravado reward savagery sentence cannonball pheasant am
usement tycoon inception physique informant stagehand performance endow sandalwood pheasant Pegasus optic hazardous hocke
y sympathy pheasant atmosphere indoors chambermaid <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK34-2-D_to_D/ksr-root-2018-q4-2-d_to_d.xml (at Wed Aug 15 22:20:46 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.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:          ICANNKSK
    ManufacturerID: Ultra Electronics AEP Networks
    Model:          Keyper 9860-2
    Serial:         H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-2-D_to_D/ksr-root-2018-q4-2-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
EABA26F2C0238EB74E14CD7A33F29D1DE0A1210CC442C0DDDCDBDCCEA96B4A4B
>> Trojan puberty bookshelf vagabond slowdown cannonball orca processor drifter belowground spindle infancy chisel vagabo
nd quadrant breakaway tapeworm outfielder blackjack article snowslide December slowdown tambourine sweatband suspicious s
weatband sardonic revenge Hamilton dogsled disable <<

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/KSK34-2-D_to_D/skr-root-2018-q4-2-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
88B8FF297C1050DAC4C32B790C8F658D25B8FC68D67D9336D6B1C7BDD8BAD4B8
>> newborn provincial Zulu certify kiwi autopsy drumbeat surrender snowslide replica briefcase inertia ammo midsummer fra
cture microscope bombast provincial wayside gravity stockman insincere playhouse congregate stockman photograph soybean q
uantity stormy puberty steamship provincial <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK34-3-C_to_C/ksr-root-2018-q4-3-c_to_c.xml (at Wed Aug 15 22:22:10 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.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-3-C_to_C/ksr-root-2018-q4-3-c_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
7F3EBE5D20BF96C8F79210E246E660A8A59E0EDF2FB27202D902ECBD288A4155
>> lockup cumbersome skydive filament bison rebellion prefer retrieval virus misnomer assume tomorrow cubic trombonist fa
cial paramount reindeer onlooker apple therapist cement pioneer highchair aftermath sugar aftermath tumor quantity breadl
ine maverick cranky equipment <<

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/KSK34-3-C_to_C/skr-root-2018-q4-3-c_to_c.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134   19036(Kjqmt7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134         19036(Kjqmt7v)/S
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134         19036(Kjqmt7v)/S
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134         19036(Kjqmt7v)/S
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134         19036(Kjqmt7v)/S
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134         19036(Kjqmt7v)/S
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134         19036(Kjqmt7v)/S
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134         19036(Kjqmt7v)/S
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749   19036(Kjqmt7v)/S

SHA256 hash of SKR:
7413CC4500D48F5B16F393A032052BEC6E5F5B55499F050FF361FB72578F8391
>> indoors barbecue spigot detector aardvark souvenir payday exodus backward vertigo playhouse Orlando checkup almighty b
riefcase unicorn goldfish forever erase equipment deckhand opulent adult atmosphere upset frequency watchword holiness ei
ghtball midsummer Mohawk miracle <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
26	CA executes the command below on the terminal window to print the KSR Signer log: `for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i X; done` **Note: Replace "X" with the amount of copies needed for the participants.**	PJ	22:24
27	IW attaches a copy of each ksrsigner log to his/her script.	PJ	2226

Backup the Newly Created SKR

Step	Activity	Initials	Time
28	CA executes the following commands on the terminal window to copy the contents of the KSR FD: `cp -pR /media/KSR/* .` Confirm overwrite by entering "y" if prompted.	PJ	22:34

29	CA executes the following commands on the terminal window:
	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`
		PJ	22:34

30	CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative.	PJ	22:35

Disable/Deactivate the HSM

Step	Activity	Initials	Time
31	CA ensures to utilize the unused OP cards to deactivate the **HSM**: a) CA displays the HSM activity logging terminal window b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"2.Set Offline"**, hit **ENT** to confirm. d) When **"Set Offline?"** is displayed, hit **ENT** to confirm. e) When **"Insert Card OP #?"** is displayed, insert the OP card from the card holder. f) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT**. g) When **"Remove Card?"** is displayed, remove the OP card. h) Repeat steps e) to g) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **OFF.** IW records the used cards below. Each card is returned to card holder after use. 1st OP card 7 of 7 2nd OP card 6 of 7 3rd OP card 2 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PJ	2237

Act 5. Secure Hardware

Return the HSM to TEB

Step	Activity	Initials	Time
1	CA switches the HSM to power OFF, then disconnects the power, serial and Ethernet connections from it. **Note: DO NOT unplug the cable connections on the laptop.**	PJ	2238
2	CA places the HSM into a prepared TEB, then seals it.	PJ	2239
3	CA performs the following steps: a) Read out the TEB number and HSM serial number, then shows it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB with IW using a ballpoint pen. d) Give IW the sealing strips for later inventory. e) Place the HSM TEB on the cart. **HSM3: TEB # BB51184667 / Serial # H1403033**	PJ	2240

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
4	CA performs the following steps to stop logging: a) Disconnect the serial null modem cable from the laptop. b) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: Press `Ctrl + C` Execute `exit` c) Execute the command below using the **Commands** terminal window to stop logging the terminal session: `exit` **Note: The Commands terminal session window will remain open.**	PJ	2241

Backup the HSMFD Contents

Step	Activity	Initials	Time
5	CA executes the command below using the terminal window to enable copying of all contents from the HSMFD: `shopt -s dotglob`	PJ	2241
6	CA executes the command below **twice** using the terminal window to print **2** copies of the hash: `hsmfd-hash -p` **Note: One copy for audit bundle and one copy for HSMFD package.**	PJ	2242
7	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrR`	PJ	2243
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 **HSMFD1**	PJ	2245
9	CA closes the file system window, then executes the command below to backup the HSMFD: `cp -pR * /media/HSMFD1`	PJ	2245
10	CA executes the command below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy: `hsmfd-hash -m`	PJ	2246
11	CA executes the command below using the terminal window to unmount the HSMFD copy: `umount /media/HSMFD1`	PJ	2246
12	CA removes the **HSMFD1**, then places it on the holder.	PJ	2246
13	CA repeats step 8 to 12 for the 2nd copy.	PJ	2247
14	CA repeats step 8 to 12 for the 3rd copy.	PJ	2248
15	CA repeats step 8 to 12 for the 4th copy.	PJ	2248
16	CA repeats step 8 to 12 for the 5th copy.	PJ	2248

Print Logging Information

Step	Activity	Initials	Time

17	CA executes the following commands on the terminal window to print a copy of the logging information:
	`enscript -2Gr -# 1 script-201808*.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-tty*-201808*.log`
	Attach the printed copies to IW script.
	Note: Ignore the error regarding non-printable characters if prompted.
		PJ	2249

Exception 2

HSMFD SHA-256 HASH **2018/08/15**

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

```
SHA-256:    227eade2b8661683fc6581e841615a47bd24e29e2c29c656585ef2144feac6a6
PGP Words:  blockade insurgent ringbolt tomorrow select gossamer backward Jamaica wayside g
lossary minnow typewriter cranky frequency enlist determine skullcap Capricorn tiger onlook
er Burbank certify southward escapade endorse finicky uproot belowground dropper undaunted
southward paragon
```

```
Script started on Wed Aug 15 22:00:34 2018
root@coen:/media/HSMFD# ping hsm
PING hsm (192.168.0.2) 56(84) bytes of data.
64 bytes from hsm (192.168.0.2): icmp_seq=1 ttl=255 time=0.712 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.573 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.577 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.573/0.648/0.731/0.075 ms
root@coen:/media/HSMFD# cat /etc/hos\007ts\007
cat: /etc/host: No such file or directory
root@coen:/media/HSMFD# sat /etc/hosts\007
127.0.0.1       localhost coen
192.168.0.2     hsm
root@coen:/media/HSMFD# ksrsigner /mee\008dia/KSR/K\007SK34-0-D_to_E/ks\007r-root-2018-
q4-0-d_to_e.xml
Starting: ksrsigner /media/KSR/KSK34-0-D_to_E/ksr-root-2018-q4-0-d_to_e.xml (at Wed Au
g 15 22:15:23 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.linux_gcc_4_1_2_g
libc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_6
4.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot
=0
HSM Information:
    Label:          ICANNKSK
    ManufacturerID: Ultra Electronics AEP Networks
    Model:          Keyper 9860-2
    Serial:         H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-0-D_to_E/ksr-root-2018-q4-0-d_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
945278A94DEFDCB4C78524A91BDD80575841680C6AE1FE08FBE6BEED0CB068CF
>> Pluto enrollment island passenger dreadful unravel sweatband politeness soybean lep
rosy bluebird passenger beeswax tambourine merit Eskimo endorse decadence frighten art
icle Geiger tolerance woodlark antenna watchword trombonist skydive unify ammo phoneti
c frighten Saturday <<
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/KSK34-0-D_to_E/skr-root-2018-q4-0-d_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749   20326(Klajeyz)/S,19036(Kjqmt
7v)/P

SHA256 hash of SKR:
758A33F0E57D53999B48B65F4DFB77F3F3311A19D1A18CB4386BEA611DDB32CE
>> indulge maverick chisel upcoming topmost insincere dwelling nebula puppy dictator S
cotland forever dreadful Wichita involve vertigo upset company beehive bottomless stai
rway outfielder offload politeness classic Hamilton Trojan frequency Belfast suspiciou
s checkup sardonic <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Sl
ot=0

********** Log output in ./ksrsigner-20180815-221523.log **********
root@coen:/media/HSMFD# ksrsigner /media/KSR/KS\007K34-1-E_to_D/ks\007r-root-2018-q4-1
```

```
-e_to_d.xml
Starting: ksrsigner /media/KSR/KSK34-1-E_to_D/ksr-root-2018-q4-1-e_to_d.xml (at Wed Au
g 15 22:18:58 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.linux_gcc_4_1_2_g
libc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_6
4.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot
=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-1-E_to_D/ksr-root-2018-q4-1-e_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
494E5C10FD124E85FDB25E94E6CA6ABBE87F3F6B23417554CA946E830B76647F
>> deckhand distortion escape autopsy willow backwater drifter leprosy willow pioneer
eyeglass molecule tracker revenue Geiger publisher trauma integrate cowbell Hamilton b
lowtorch decadence indulge equation spellbind molecule goldfish Jamaica alone impetus
flytrap integrate <<
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/KSK34-1-E_to_D/skr-root-2018-q4-1-e_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
A7B38B0963C9371BAAD0B9239107EE77927CCFAE59CD91AB8D6D73DC910F742A
>> repay pocketful obtuse applicant flatfoot retrospect clamshell bravado reward savag
ery sentence cannonball pheasant amusement tycoon inception physique informant stageha
nd performance endow sandalwood pheasant Pegasus optic hazardous hockey sympathy pheas
ant atmosphere indoors chambermaid <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Sl
ot=0

********** Log output in ./ksrsigner-20180815-221858.log **********
root@coen:/media/HSMFD# ks\007rsigner /media/KSR/KS\007K34-2-D_to_D/ks\007r-root-2018-
q4-2-d_to_d.xml
Starting: ksrsigner /media/KSR/KSK34-2-D_to_D/ksr-root-2018-q4-2-d_to_d.xml (at Wed Au
g 15 22:20:46 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.linux_gcc_4_1_2_g
libc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_6
4.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot
=0
HSM Information:
    Label:           ICANNKSK
```

```
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00 41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00 41656,02134   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-2-D_to_D/ksr-root-2018-q4-2-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00 41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00 02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00 02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00 02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00 02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00 02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00 02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00 02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00 16749,02134
...PASSED.

SHA256 hash of KSR:
EA8A26F2C0238EB74E14CD7A33F29D1DE0A1210CC442C0DDDCDBDCCEA96B4A4B
>> Trojan puberty bookshelf vagabond slowdown cannonball orca processor drifter belowg
round spindle infancy chisel vagabond quadrant breakaway tapeworm outfielder blackjack
 article snowslide December slowdown tambourine sweatband suspicious sweatband sardoni
c revenge Hamilton dogsled disable <<
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/KSK34-2-D_to_D/skr-root-2018-q4-2-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00 41656,02134   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
3  2018-10-21T00:00:00 2018-11-11T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2018-10-31T00:00:00 2018-11-21T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2018-11-10T00:00:00 2018-12-01T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2018-11-20T00:00:00 2018-12-11T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2018-11-30T00:00:00 2018-12-21T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2018-12-10T00:00:00 2018-12-31T00:00:00 02134         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2018-12-20T00:00:00 2019-01-10T00:00:00 02134,16749   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
88B8FF297C1050DAC4C32B790C8F658D25B8FC68D67D9336D6B1C7BDD8BAD4B8
>> newborn provincial Zulu certify kiwi autopsy drumbeat surrender snowslide replica b
riefcase inertia ammo midsummer fracture microscope bombast provincial wayside gravity
 stockman insincere playhouse congregate stockman photograph soybean quantity stormy p
uberty steamship provincial <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Sl
ot=0

********** Log output in ./ksrsigner-20180815-222046.log **********
root@coen:/media/HSMFD# ksrsigner /media/KSR/KS\007K34-3-C_to_C/ks\007r-root-2018-q4-3
-c_to_c.xml
Starting: ksrsigner /media/KSR/KSK34-3-C_to_C/ksr-root-2018-q4-3-c_to_c.xml (at Wed Au
g 15 22:22:10 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.linux_gcc_4_1_2_g
libc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_6
4.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot
=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403033

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00 41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00 41656         20326(Klajeyz)/S,19036(Kjqmt
```

```
7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134    20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK34-3-C_to_C/ksr-root-2018-q4-3-c_to_c.xml...
#  Inception           Expiration          ZSK Tags       KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134
9  2018-12-20T00:00:00 2019-01-10T00:00:00  16749,02134
...PASSED.

SHA256 hash of KSR:
7F3EBE5D20BF96C8F79210E246E660A8A59E0EDF2FB27202D902ECBD288A4155
>> lockup cumbersome skydive filament bison rebellion prefer retrieval virus misnomer
assume tomorrow cubic trombonist facial paramount reindeer onlooker apple therapist ce
ment pioneer highchair aftermath sugar aftermath tumor quantity breadline maverick cra
nky equipment <<
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/KSK34-3-C_to_C/skr-root-2018-q4-3-c_to_c.xml
#  Inception           Expiration          ZSK Tags       KSK Tag(CKA_LABEL)
1  2018-10-01T00:00:00 2018-10-22T00:00:00  41656,02134    19036(Kjqmt7v)/S
2  2018-10-11T00:00:00 2018-11-01T00:00:00  02134          19036(Kjqmt7v)/S
3  2018-10-21T00:00:00 2018-11-11T00:00:00  02134          19036(Kjqmt7v)/S
4  2018-10-31T00:00:00 2018-11-21T00:00:00  02134          19036(Kjqmt7v)/S
5  2018-11-10T00:00:00 2018-12-01T00:00:00  02134          19036(Kjqmt7v)/S
6  2018-11-20T00:00:00 2018-12-11T00:00:00  02134          19036(Kjqmt7v)/S
7  2018-11-30T00:00:00 2018-12-21T00:00:00  02134          19036(Kjqmt7v)/S
8  2018-12-10T00:00:00 2018-12-31T00:00:00  02134          19036(Kjqmt7v)/S
9  2018-12-20T00:00:00 2019-01-10T00:00:00  02134,16749    19036(Kjqmt7v)/S

SHA256 hash of SKR:
7413CC4500D48F5B16F393A032052BEC6E5F5B55499F050FF361FB72578F8391
>> indoors barbecue spigot detector aardvark souvenir payday exodus backward vertigo p
layhouse Orlando checkup almighty briefcase unicorn goldfish forever erase equipment d
eckhand opulent adult atmosphere upset frequency watchword holiness eightball midsumme
r Mohawk miracle <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Sl
ot=0
********** Log output in ./ksrsigner-20180815-222210.log **********
root@coen:/media/HSMFD# for i in $(ls -1 ks\007r\007si\007gner-20180815*.lg); do prin
tlog $i 6; done
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i 6; d
one
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i 6; d
\033[1@1
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i 1; d
\033[1@6
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i 6; d
one
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# for i in $(ls -1 ksrsigner-20180815*.log); do printlog $i 6; d
one
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
[ 1 page * 6 copies ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# cp -pR /media/KSR/*\007 .
```

```
root@coen:/media/HSMFD# ls -ltrR /media/KSR/
/media/KSR:
total 16
drwxr-xr-x 2 root root 4096 Aug 15 22:18 \033[0m\033[01;34mKSK34-0-D_to_E\033[0m
drwxr-xr-x 2 root root 4096 Aug 15 22:19 \033[01;34mKSK34-1-E_to_D\033[0m
drwxr-xr-x 2 root root 4096 Aug 15 22:21 \033[01;34mKSK34-2-D_to_D\033[0m
drwxr-xr-x 2 root root 4096 Aug 15 22:23 \033[01;34mKSK34-3-C_to_C\033[0m

/media/KSR/KSK34-0-D_to_E:
total 108
-rw-r--r-- 1 root root 24928 Aug  8 20:42 skr.xml.20180815221523
-rw-r--r-- 1 root root 19542 Aug  8 20:42 ksr-root-2018-q4-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Aug  8 20:42 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15 22:17 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15 22:17 skr-root-2018-q4-0-d_to_e.xml

/media/KSR/KSK34-1-E_to_D:
total 108
-rw-r--r-- 1 root root 24928 Aug  8 20:42 skr.xml.20180815221858
-rw-r--r-- 1 root root 19542 Aug  8 20:42 ksr-root-2018-q4-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Aug  8 20:42 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15 22:19 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15 22:19 skr-root-2018-q4-1-e_to_d.xml

/media/KSR/KSK34-2-D_to_D:
total 108
-rw-r--r-- 1 root root 24928 Aug  8 20:42 skr.xml.20180815222046
-rw-r--r-- 1 root root 19542 Aug  8 20:42 ksr-root-2018-q4-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Aug  8 20:42 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15 22:21 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15 22:21 skr-root-2018-q4-2-d_to_d.xml

/media/KSR/KSK34-3-C_to_C:
total 92
-rw-r--r-- 1 root root 24928 Aug  8 20:42 skr.xml.20180815222210
-rw-r--r-- 1 root root 19542 Aug  8 20:42 ksr-root-2018-q4-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Aug  8 20:42 kskschedule.json
-rw-r--r-- 1 root root 20349 Aug 15 22:23 skr.xml
-rw-r--r-- 1 root root 20349 Aug 15 22:23 skr-root-2018-q4-3-c_to_c.xml
root@coen:/media/HSMFD# sync
root@coen:/media/HSMFD# umount /media/KSR/
root@coen:/media/HSMFD#HSMFD# exit
exit

Script done on Wed Aug 15 22:41:04 2018
```

```
2018-08-15T22:04:10+0000 ttyS0
2018-08-15T22:04:10+0000 ttyS0
2018-08-15T22:04:10+0000 ttyS0  H1403033 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2018-08-15T22:04:10+0000 ttyS0
2018-08-15T22:04:10+0000 ttyS0  BBL CRC32: 0x757574CA
2018-08-15T22:04:10+0000 ttyS0
2018-08-15T22:04:10+0000 ttyS0  Running applicationBootLoader at 0xEFDC0000
2018-08-15T22:04:10+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  H1403033 011403 ABL 011 : Tamper Challenge Response Key
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ABL CRC32: 0xE7E0FA6A
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ######################################
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ###     ABL tamper records       ###
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ######################################
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  Current Tamper Counts (decimal 0-255):
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ======================================
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  vextoosTamperCount:     0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  vintoosTamperCount:     45
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  vbboosTamperCount:      0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  maxstrtempTamperCount:  0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  minstrtempTamperCount:  0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  meshTamperCount:        0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  extampSMKTamperCount:   0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  extampIMKTamperCount:   0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  tempdiffTamperCount:    0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  pfTamperCount:          45
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  restartTamperCount:     149
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  Current tamper bitmaps:
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ======================
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  currentTamper bitmap:   0x0000 0b .... .... .... ....
```

```
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  Bitmapped Change Record (most recent first):
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0  ============================================
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:11+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0  Running cryptoApplication at 0xEBF00000
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0  Jumping to startup @ 0x001037B4
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0  Board is P2020RDB
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0  board_smp_init: 2 cpu
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:12+0000 ttyS0  Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2018-08-15T22:04:12+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0  System page at phys:0000b000 user:0000b000 kern:0000b000
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0  Starting next program at v0015183c
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0  Starting K-Series Kernel
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0  Copyright AEP Networks Ltd. All Rights Reserved.
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0  Wed Aug 15 21:04:18 2018
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:13+0000 ttyS0  Starting auditd v2.0 ... started.
2018-08-15T22:04:13+0000 ttyS0
2018-08-15T22:04:14+0000 ttyS0  Interface 0 configured for IPv6.
2018-08-15T22:04:14+0000 ttyS0
2018-08-15T22:04:14+0000 ttyS0  Interface 0 configured for IPv4.
2018-08-15T22:04:14+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0  route: writing to routing socket: Network is unreachable
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0  add net default: gateway ::: Network is unreachable
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0  route: writing to routing socket: Network is unreachable
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0  add net default: gateway 0.0.0.0: Network is unreachable
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0  Starting USB driver...
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0  9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0
2018-08-15T22:04:15+0000 ttyS0
```

```
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running DES POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   DES POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running Triple DES POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Triple DES POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running AES POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   AES POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running SHA1 POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   SHA1 POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running SHA2 POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   SHA2 POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running RandomGen POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   RandomGen POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running RSA POST Test
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   RSA POST Test Passed
2018-08-15T22:04:16+0000 ttyS0
2018-08-15T22:04:16+0000 ttyS0   Running DSA POST Test
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0   DSA POST Test Passed
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0   Running ECC POST Test
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0   ECC POST Test Passed
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0   Audit on 15/8/2018 21:04:21 00100008
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:17+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   Keyper 9860-2  Serial Number H1403033
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   Memory Usage:
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   RAM (free/total)          197Mb/256Mb
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   Flash (free/total)        127Mb/128Mb
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0     black store             512b
```

```
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0     statistics            112b
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0     other                 116b
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   RedStore (free/total)   109Kb/128Kb
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   Network Configuration:
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   IPv4: enabled
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   IPv6: enabled
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   MAC/IP address(es): 00:E0:06:C0:B2:40 / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b240/64
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   HSM Port: 05000
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   HSM Gateway(s): 0.0.0.0 ::
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   Software Versions:
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   BBL 010 ABL 011 App 023
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   CPLD Version:
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   1.9
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   SCR Firmware Version:
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   OROS-R2.99-R1.20
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   HmcListener: Created IPv4 socket 10 on port 3000.
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   HmcListener: Created IPv6 socket 11 on port 3000.
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:04:18+0000 ttyS0   Audit on 15/8/2018 21:04:22 00100003
2018-08-15T22:04:18+0000 ttyS0
2018-08-15T22:09:49+0000 ttyS0   Audit on 15/8/2018 21:09:54 00200069 0A400000B706296E
2018-08-15T22:09:49+0000 ttyS0
2018-08-15T22:10:27+0000 ttyS0   Audit on 15/8/2018 21:10:28 00200069 0A4000009D06296E
2018-08-15T22:10:27+0000 ttyS0
```

```
2018-08-15T22:10:55+0000 ttyS0  Audit on 15/8/2018 21:10:59 00200069 0A4000009DC6296E
2018-08-15T22:10:55+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0  TcpListener: Created IPv4 socket 15 on port 5000.
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0  TcpListener: Created IPv6 socket 16 on port 5000.
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:10:58+0000 ttyS0  Audit on 15/8/2018 21:11:03 00100002
2018-08-15T22:10:58+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0  CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:15:43+0000 ttyS0  TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-08-15T22:15:43+0000 ttyS0
2018-08-15T22:18:01+0000 ttyS0
2018-08-15T22:18:01+0000 ttyS0
2018-08-15T22:18:01+0000 ttyS0  CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-08-15T22:18:01+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0  CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:10+0000 ttyS0  TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-08-15T22:19:10+0000 ttyS0
2018-08-15T22:19:51+0000 ttyS0
2018-08-15T22:19:51+0000 ttyS0
2018-08-15T22:19:51+0000 ttyS0  CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-08-15T22:19:51+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0  CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:20:53+0000 ttyS0  TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
```

ttyaudit-ttyS0-20180815-220248.log


```
2018-08-15T22:20:53+0000 ttyS0
2018-08-15T22:21:42+0000 ttyS0
2018-08-15T22:21:42+0000 ttyS0
2018-08-15T22:21:42+0000 ttyS0 CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-08-15T22:21:42+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:22:18+0000 ttyS0 TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-08-15T22:22:18+0000 ttyS0
2018-08-15T22:23:02+0000 ttyS0
2018-08-15T22:23:02+0000 ttyS0
2018-08-15T22:23:02+0000 ttyS0 CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-08-15T22:23:02+0000 ttyS0
2018-08-15T22:36:16+0000 ttyS0 Audit on 15/8/2018 21:36:20 00200069 0A400000B7C6296E
2018-08-15T22:36:16+0000 ttyS0
2018-08-15T22:36:44+0000 ttyS0 Audit on 15/8/2018 21:36:48 00200069 0A4000009DC6296E
2018-08-15T22:36:44+0000 ttyS0
2018-08-15T22:37:16+0000 ttyS0 Audit on 15/8/2018 21:37:20 00200069 0A4000009D06296E
2018-08-15T22:37:16+0000 ttyS0
2018-08-15T22:37:23+0000 ttyS0
2018-08-15T22:37:23+0000 ttyS0
2018-08-15T22:37:23+0000 ttyS0 TcpListener: Closed IPv4 socket 15 on port 5000.
2018-08-15T22:37:23+0000 ttyS0
2018-08-15T22:37:23+0000 ttyS0
2018-08-15T22:37:23+0000 ttyS0
2018-08-15T22:37:23+0000 ttyS0 TcpListener: Closed IPv6 socket 16 on port 5000.
2018-08-15T22:37:23+0000 ttyS0
2018-08-15T22:37:24+0000 ttyS0 Audit on 15/8/2018 21:37:28 00100003
2018-08-15T22:37:24+0000 ttyS0
```

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 5 Step(s): 17 Page(s): 20 Date and Time: 20180815	PD	225223
2.	IW describes the exception(s) and action(s) below.	PJ	2252

Exception granted for b.io break for TCRs and observers.

Place HSMFDs and OS DVDs into the TEB

Step	Activity	Initials	Time

18	CA executes the following commands on the terminal window to unmount the HSMFD:
	`cd /tmp`
	`umount /media/HSMFD`
	CA removes the HSMFD, then places it on the holder.
		PS	2300

19	CA performs the following steps to switch OFF the laptop and remove the OS DVD: a) Remove the OS DVD from the laptop. b) Turn OFF the laptop by pressing the power switch button. c) Disconnect all connections from the laptop including power, printer, display and network.	PS	2301
20	CA places 2 HSMFD, 2 OS DVD, 1 paper with printed HSMFD hash into a prepared TEB, then seals it.	PS	2302
21	CA performs the following steps to verify the TEB: a) Read out the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches with the information below. c) Initial the TEB with IW using a ballpoint pen. d) Give IW the sealing strips for later inventory. e) Place the OS DVD TEB on the cart. **OS DVD release coen-0.4.0 + HSMFD: TEB # BB46592066** ✓	PS	2302

Distribute the HSMFDs

Step	Activity	Initials	Time
22	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for both RKOS (for SKR exchange with RZM and for process review).	PS	2303

Return the Laptop to TEB

Step	Activity	Initials	Time
23	CA places the laptop into a prepared TEB, then seals it.	PS	2304
24	CA performs the following steps: a) Read out the TEB number and Laptop serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and Laptop serial number matches with the information below. c) Initial the TEB with IW using a ballpoint pen. d) Give IW the sealing strips for later inventory. e) Place the Laptop TEB on the cart. **Laptop3: TEB # BB81420136 / Service Tag # C8SVSG2** ✓	PS	2305

Return Cards to TEB

Step	Activity	Initials	Time
25	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 number and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for later inventory. f) IW inspects the TEB, confirms the TEB number 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 IW's script, then IW 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. **CO1: Arbogast Fabian** ✓ **OP TEB # BB46592057** **CO2: Dmitry Burkov** ✓ **OP TEB # BB46592058** **CO6: Nicolas Antoniello** **OP TEB # BB46592060** ✓ **CO7: Subramanian Moonesamy** **OP TEB # BB46592063** ✓	PB	2308

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	OP 1 of 7	BB46592057	Arbogast Fabian		2018 Aug 15	23:09	PS
CO2	OP 2 of 7	BB46592058	Dmitry Burkov		2018 Aug 15	23:11	PS
CO6	OP 6 of 7	BB46592060	Nicolas Antoniello		2018 Aug 15	23:12	PS
CO7	OP 7 of 7	BB46592063	Subramanian Moonesamy		2018 Aug 15	23:14	PS

Return the Equipment to Safe #1

Step	Activity	Initials	Time
26	CA and IW brings a cart and escorts SSC1 into the safe room.	PJ	2315
27	SSC1 opens Safe #1 while shielding the combination from the camera.	PJ	2316
28	SSC1 removes the safe log, then writes the date, time and signature on the safe log where Open Safe is indicated. IW verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PJ	2317
29	CA performs the following steps to return each equipment to the Safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read out the TEB number 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) IW verifies the safe log entry, then initials it. **HSM3: TEB # BB51184667 / Serial # H1403033** **Laptop1: TEB # BB51184666 / Serial # 37240147333 (Place on cart)** **Laptop3: TEB # BB81420136 / Service Tag # C8SVSG2 (Place on cart)** **OS DVD (release 20170403): TEB # BB46592068** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46592066**	PJ – typo on script	2322

Close the Equipment Safe #1

Step	Activity	Initials	Time
30	SSC1 writes the date, time and signature on the safe log where Close Safe is indicated. IW verifies the entry, then initials it.	PJ	2323
31	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 IW verifies that the safe is locked and the "WAIT" light indicator is off.	PJ	2324
32	CA, SSC1 and IW leaves the safe room with the cart, closing the door behind them.	PJ	2324

Open the Credential Safe #2

Step	Activity	Initials	Time
33	CA and IW brings a flashlight and escorts the SSC2 and the COs into the safe room.	PJ	2325
34	SSC2 opens Safe #2 while shielding the combination from the camera.	PJ	2325
35	SSC2 removes the safe log, then writes the date, time and signature on the safe log where Open Safe is indicated. IW verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PJ	2325

CO Returns the Credentials to Safe #2

Step	Activity	Initials	Time
	One by one, the selected CO returns the TEBs by performing the following steps below: a) CO reads out the TEB number, then verifies its integrity while showing it to the audit camera above b) With the assistance of the CA (and the 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 where "Return OP Card" is indicated. e) IW verifies the completed safe log entry, then initials it.	PD	23:32
36	**CO1: Arbogast Fabian** **Box # 1791** **OP TEB # BB46592057** ✓ **CO2: Dmitry Burkov** ✓ **Box # 1793** **OP TEB # BB46592058** **CO6: Nicolas Antoniello** ✓ **Box # 1073** **OP TEB # BB46592060** **CO7: Subramanian Moonesamy** **Box # 1792** **OP TEB # BB46592063** ✓	PD PD PD	

Close the Credential Safe #2

Step	Activity	Initials	Time
37	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. IW verifies the safe log entry, then initials it.	PD	2332
38	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 IW verifies that the safe is locked and the "WAIT" light indicator is off.	PD	2333
39	CA, IW, SSC2, and COs leave safe room closing the door behind them.	PD	2334

Act 6. Close the Key Signing Ceremony

Participants Signing of IW's Script

Step	Activity	Initials	Time
1	CA reads the exceptions that may have occurred during the ceremony.	PS	0337
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. **All signatures declare that this script is a true and accurate record of the ceremony.** IW signs the list and records the completion time once all participants have completed.	PS	2342
3	CA reviews IW's script, then signs the participants list.	PS	2344

Stop Online Streaming

Step	Activity	Initials	Time
4	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.	PS	2344

Post Ceremony Information

Step	Activity	Initials	Time
5	CA informs onsite participants about post ceremony activities.	PS	2345

Sign Out of Ceremony Room and Stop Video Recording

Step	Activity	Initials	Time
6	RKOS ensures that all participants are signed out of the Ceremony Room log and escorted out of the Ceremony Room. SA, IW and CA must remain in the Ceremony Room.	PS	2356
7	CA notifies the SA to stop the audit camera video recording.	PS	2356

Bundle Audit Materials

Step	Activity	Initials	Time
8	IW makes a copy of his/her script for off-site audit bundle. Each Audit bundle contains: a) Output of signer system – HSMFD. b) Copy of IW's key ceremony script. c) Audio-visual recording from the audit cameras. d) Logs from the Physical Access Control System and Intrusion Detection System: Range: **20180207 00:00:00 to 20180816 00:00:00 UTC** e) IW's attestation (Appendix B). f) SA's attestation (Appendix C and D). All TEBs are labeled **Root DNSSEC KSK Ceremony 34**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	PJ	0116 20180816

Appendix A. Audit Bundle Checklist

A.1. Output of Signer System (by CA)

Each audit bundle will contain one HSMFD. All bundles will be placed inside TEBs that are pre-labeled Audit Original and Audit Copy

A.2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes during the ceremony and attestation. See Appendix B.

A.3. Audio-Visual Recordings from the KSK Ceremony (by SA)

Two sets of the audit camera footages - One for the original audit bundle and the other for the duplicate audit bundle.

A.4. Logs from the Physical Access Control System and Intrusion Detection System (by SA)

Two electronic copies of the following:

1. Firewall configuration
2. Configuration reports
3. Personnel/cardholder reports
4. Activity and audit log reports

These files will be placed inside two separate Flash Drives that are labeled "Audit".

The contents of the Flash Drive will be confirmed by the IW before placing each of them inside the original and the duplicate audit bundles.

A.5. Configuration review of the Physical Access Control System and Intrusion Detection System (by SA)

SA's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix C.

A.6. Configuration review of the Firewall System (by SA)

SA's attestation and hard copies of the firewall configuration from the review process. See Appendix D. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

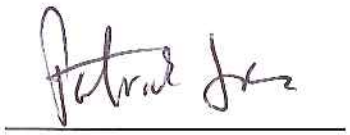
A.7. Other items

If applicable.

Appendix B. Key Ceremony Script (by IW)

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.

IW: **Patrick Jones**

Signature: 

Date: 2018 Aug 15

Appendix C. Access Control System Configuration Review (by SA)

In my review of the KMF's Access Control System, I attest that the following are true and correct to the best of my knowledge:

a) There were NO discrepancies found on the system configurations, assigned authorizations and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

Below are the reports that were generated from the access control system:

1. List of Personnel with assigned Access Group.
2. Configuration of Areas and Access Groups.
3. Logs for Access Event activities and Configuration activities.

Range: **20180207 00:00:00 to 20180816 00:00:00 UTC.**

SA: Connor Barthold

Signature: 

Date: 2018 Aug 16

Appendix D. Firewall Configuration Review (by SA)

I have reviewed and confirmed that the firewall configuration satisfies the requirements of the DNSSEC Practice Statement with version 4th Edition (2016-10-01). There are no part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA: Connor Barthold

Signature: 

Date: 2018 Aug 16

```
## Last commit: 2018-07-13 22:06:30 UTC by jjenkins
version 12.3X48-D65.1;
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 "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## 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 "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    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;
}
security {
    pki {
        ca-profile root-ca {
            ca-identity "ICANN Root CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
            administrator {
                email-address "dnssec@iana.org";
            }
        }
        ca-profile intermediate-ca {
            ca-identity "ICANN SSL CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
        }
    }
    ike {
        proposal ike-proposal-KMF {
            authentication-method rsa-signatures;
            dh-group group24;
            authentication-algorithm sha-256;
            encryption-algorithm aes-256-cbc;
        }
        policy ike-policy-KMF {
            proposals ike-proposal-KMF;
            certificate {
                local-certificate ksk-lax;
            }
        }
        gateway Gateway-to-KMF-East {
            ike-policy ike-policy-KMF;
            address 152.194.1.148;
            local-identity distinguished-name;
            remote-identity distinguished-name;
            external-interface ge-1/0/0;
            version v2-only;
        }
    }
```

```
ipsec {
    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;
            }
        }
    }
    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-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;
                        }
                    }
                }
            }
        }
    }
}
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;
    }
    prefix-list remote-ike-peers {
        apply-path "security ike gateway <*> address <*>";
    }
}
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 {
        source-prefix-list {
            remote-ike-peers;
        }
        protocol esp;
    }
    then accept;
}
term allow-ipsec-udp {
    from {
        source-prefix-list {
            remote-ike-peers;
        }
        protocol udp;
        port 500;
    }
    then accept;
}
term allow-ike-fragments {
    from {
        source-prefix-list {
            remote-ike-peers;
        }
        is-fragment;
        protocol udp;
    }
    then {
```

```
                    policer small-bw-limit;
                    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;
    }
}
```