Root DNSSEC KSK Ceremony 35

Thursday November 15, 2018

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

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	Francisco Arias / ICANN		2018 Nov 15	21:06
IW	Shauna Royston / ICANN			
SSC1	James Cole / ICANN			
SSC2	Carlos Reyes / ICANN			
CO4	Robert Seastrom			
CO5	Christopher Griffiths			
CO6	Gaurab Upadhaya			
~~RZM~~	~~Ryan Brown / Verisign~~			
~~RZM~~	~~Eric Matthews / Verisign~~			
~~RZM~~	~~Wali Farhad / Verisign~~			
AUD	Jun Lin / RSM			
AUD	Matthew Kleckner / RSM			
SA	Reed Quinn / ICANN			
SA	Patrick Tudor / ICANN	P. TUDOR		
RKOS / CA Backup	Andres Pavez / PTI			
IW Backup	David Prangnell / 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.

Instructions for Root DNSSEC KSK Ceremony

The Root DNSSEC Key Signing Key (KSK) Ceremony is a scripted meeting where individuals with specific roles generate, or access the private key component of the Root Zone DNSSEC KSK. The process is audited by a third party firm for compliance with SOC 3 framework. The script and recordings are published online for the wider Internet community to review.

Ceremony Guidelines:

- 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
- Ceremony participants follow the script step by step
- CA reads each step aloud prior to its performance
- Upon completion of each step, IW announces the time of completion and records the completion time and initials their copy of the script
- Ceremony participants who notices a problem or an error during the ceremony should interrupt the ceremony. Ceremony participants agree on a resolution before proceeding
- Questions and suggestions for improvement are welcome and can be discussed at any time or after the ceremony during the ceremony debrief

Unplanned events **(exceptions)** during the ceremony are evaluated, documented, and acted upon. It is the CA's sole responsibility to decide on proper actions after consulting with the IW. In either case, an exception is regarded as an incident, and incident handling procedures are enacted.

Key Management Facility Tiers:

- Tiers 1-3: Consist of the facility areas between the outside environment and the Key Ceremony Room
- Tier 4: Consists of the Key Ceremony Room and is subject to dual occupancy
- Tier 5: Consists of the Safe Room (a cage inside the Key Ceremony Room) and is subject to dual occupancy
- Tier 6: Consists of Safe 1 (Equipment Safe) and Safe 2 (Credentials Safe)
- Tier 7: Consists of the HSM stored in Safe 1 (Equipment Safe) and the safe deposit boxes installed in Safe 2 (Credentials Safe)

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:

Character	Code Word	Pronunciation
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

The CA initiates the ceremony by performing the steps below:

- Verify that the audit cameras are recording and the online video streaming is enabled
- Confirm that all the ceremony attendees have signed in on the Ceremony Room log
- Review emergency evacuation procedures
- Explain the use of personal devices and the purpose of this ceremony
- Verify the time and date so that all entries into the script follow a common timesource

Then the CA and IW will escorts the SSCs and TCRs into Tier 5 (safe room) to retrieve the equipment:

- Safe 1: HSM, laptop, OS DVD, etc
- Safe 2: The TCRs cards required to operate the HSM

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.	SR	18:00
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.	SR	18:02
3	CA asks that any new participants introduce themselves.	SR	18:02

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews the emergency evacuation procedure with onsite participants.	SR	18:03
5	CA explains the use of personal electronic devices during ceremony.	SR	18:03
6	CA briefly explains the purpose of the ceremony.	SR	18:04

Verify the Time and Date

Step	Activity	Initials	Time
7	IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2018/11/15 All entries into this script or any logs should follow this common source of time.	SR	18:05

Open the Credential Safe #2

Step	Activity	Initials	Time
8	CA and IW brings a flashlight and escorts the SSC2 and the COs into the safe room.	SR	18:06
9	SSC2 opens Safe #2 while shielding the combination from the camera.	SR	18:07
10	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.	SR	18:08

COs Extract the Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
11	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. **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584484 (Retain)** **SO TEB # BB46584596 (Check and Return)** **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46584485 (Retain)** **SO TEB # BB46584598 (Check and Return)** **CO6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB46584487 (Retain)** **SO TEB # BB21907207 (Check and Return)**		18:11 18:13 18:16 18:16

Close the Credential Safe #2

Step	Activity	Initials	Time
12	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.	SR	18:17
13	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.	SR	18:18
14	CA, IW, SSC2, and COs leave the safe room with TEBs, closing the door behind them.	SR	18:18

Open Equipment Safe #1

Step	Activity	Initials	Time
15	CA and IW brings a cart and escorts the SSC1 into the safe room.	SR	18:19
16	SSC1 opens Safe #1 while shielding the combination from the camera.	SR	18:20
17	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.	SR	18:21

Remove the Equipment from Safe #1

Step	Activity	Initials	Time
18	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 # BB51184645 / Serial # H1403032 (Check and Return)** **HSM4: TEB # BB51184628 / Serial # H1411011 (Place on cart)** **Laptop1: TEB # BB51184631 / Serial # 41593712005 (Check and Return)** **Laptop2: TEB # BB51184630 / Serial # 35063364997 (Place on cart)** **Laptop3: TEB # BB81420092 / Service Tag # J8SVSG2 (Place on cart)** **Laptop4: TEB # BB81420093 / Service Tag # 58SVSG2 (Check and Return)** **OS DVD (release 20170403) + HSMFD: TEB # BB46584489 (Place on cart)** **Note: The Service Tag # is the same as the Serial Number.**	SR SR SR	18:24 18:29 18:31

Close the Equipment Safe #1 and exit the Safe Room

Step	Activity	Initials	Time
19	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.	SR	18:31
20	SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW verifies that the safe is locked and the "WAIT" light indicator is off.	SR	18:32
21	CA, IW and SSC1 leaves the safe room with the cart, closing the door behind them.	SR	18:32

Act 2. OS DVD Acceptance Test

The CA verifies that the new operating system OS DVD matches the checksum published online at: https://github.com/iana-org/coen

The checksum is calculated using the current OS DVD and laptop. Once the new OS DVD hash has been verified it will be ready to use in production to perform the ceremony. The CA then calculates the hash of the previous ceremony HSMFD (USB flash drive that contains configuration files necessaries to perform the ceremony) and compares it to hash recorded from the Ceremony 33 annotated script. When the tests are finished the current laptop and corresponding old OS DVD will be stored in a tamper evident bag to be returned later to Safe 1.

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. **Laptop2: TEB # BB51184630 / Serial # 35063364997** **OS DVD (release 20170403) + HSMFD: TEB # BB46584489**	SR	18:37
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.	SR	18:42
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`	SR	18:45
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.	SR	18:45

OS DVD Acceptance Test

Step	Activity	Initials	Time

5	CA inserts the new **OS DVD release coen-0.4.0**[1] 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`[2] `< /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
		SR	18:50

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**	SR	18:50
7	CA repeats step 5 to 6 for the 2nd copy of the new **OS DVD release coen-0.4.0.**	SR	18:54
8	IW records his/her signature upon successful completion of the **OS DVD release coen-0.4.0** acceptance testing. Printed Name: **Shauna Royston** Signature:  Date: **2018/11/15**	SR	18:54

Verification of HSMFD Checksum

Step	Activity	Initials	Time
9	CA plugs the **Ceremony 33 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.	SR	18:55
10	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash[3] -c` IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 33 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: 67fa645fadde371c5aed318b4438b149d22eb047b7101f764d8bed3b8bff64e0 PGP Words: freedom whimsical flytrap forever ringbolt telephone clamshell Brazilian en list unify chatter Medusa crumpled consulting sailboat dinosaur standard coherence ruff led determine seabird autopsy billiard impetus dreadful Medusa tunnel councilman obtuse Yucatan flytrap tobacco	SR	18:58
11	CA executes the following commands on the terminal window to unmount the HSMFD: `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder. **Note: The verified HSMFD must be placed on the ceremony table where it is visible to the audit camera and the participants**	SR	18:59
12	CA repeats step 9 to 11 for the 2nd copy of the HSMFD.	SR	19:01

Return the OS DVDs and Laptop to TEB

Step	Activity	Initials	Time
13	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.	SR	19:02
14	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 **Laptop2** into a prepared TEB, then seals it.	SR	19:05
15	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 # BB46584688** **Laptop2: TEB # BB51184681 / Serial # 35063364997**	SR	19:07

Act 3. Setup Equipment

The CA will setup the equipment by performing the following steps:

- Boot the laptop using the OS DVD (the laptop doesn't have a hard drive)
- Setup the printer
- Verify the laptop date and time
- Format the blank flash drive that will be used to collect audit evidence
- Connect the HSMFD flash drive
- Start the log sessions
- Power on the HSM

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. **HSM4: TEB # BB51184628 / Serial # H1411011** **Laptop3: TEB # BB81420092 / Serial # J8SVSG2**	SR	19:11
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.	SR	19:17
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**	SR	19:18

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`[4]	SR	19:19

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 "20181115 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.	SR	19:20

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.	SR	19:22
7	CA repeats step 6 for the 2nd blank FD.	SR	19:23
8	CA repeats step 6 for the 3rd blank FD.	SR	19:24
9	CA repeats step 6 for the 4th blank FD.	SR	19:24
10	CA repeats step 6 for the 5th blank FD.	SR	19:25

Connect the HSMFD

Step	Activity	Initials	Time
11	CA plugs the **Ceremony 33 HSMFD** into the USB slot, then waits for it to be recognized by the OS and closes the file system window.	SR	19:26

Start the Terminal Session Logging

Step	Activity	Initials	Time
12	CA executes the command below using the terminal window to change the detault directory to HSMFD: **`cd /media/HSMFD`**	SR	19:26
13	CA executes the command below to log activities of the **Commands** terminal window: **`script script-20181115.log`**	SR	19:27

Start the HSM Activity Logging

Step	Activity	Initials	Time

14	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.
		SR	19:28

Power ON the HSM

Step	Activity	Initials	Time
15	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. **HSM4: Serial # H1411011** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	SR	19:31

Act 4. Activate HSM and Generate Signatures

Using the ksrsigner application the CA takes the Key Signing Requests (KSRs) and generates the Signed Key Responses (SKRs).

The CA activates the HSM using the TCR's cards. After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop. Then the ksrsigner application uses the private key stored in the HSM to generate the SKR. The SKR contains the digital signatures of the ZSK set to be used in the next quarter. Then the CA prints the signer log, backs up the newly created SKR and deactivates the HSM.

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. **CO4: Robert Seastrom** **OP TEB # BB46584484** **CO5: Christopher Griffiths** **OP TEB # BB46584485** **CO6: Gaurab Upadhaya** **OP TEB # BB46584487**	SR	19:34
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 4 of 7 2nd OP card 5 of 7 3rd OP card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	SR	19:37

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.	SR	19:38
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`[5] c) Wait for responses, then exit by pressing: `Ctrl + C`	SR	19:39

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).**	SR	19:41

Execute the KSR Signer for Phase E to F

Step	Activity	Initials	Time
6	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[6] `/media/KSR/KSK35-0-E_to_F/ksr-root-2019-q1-0-e_to_f.xml`	SR	19:42
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.	SR	19:43

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: ACT 1, STEP 2 8,13, Act: 4 Step(s): 18,23 Page(s): 18,19,20 6 STEP: 2 Date and Time: 2018 NOVEMBER 15 (2018/11/15)	SRL	21:04
2.	IW describes the exception(s) and action(s) below.	SRL	21:04

DUE TO UNFORESEEN WEATHER CONDITIONS IN THE NORTHEAST OF THE USA, VERISIGN, THE ROOT ZONE MAINTAINER (RZM), IS UNABLE TO ATTEND THE CEREMONY.

PER SECTION 6.7 OF THE DPS, THE VERIFICATION OF THE KSR DOCUMENT WILL BE PERFORMED WITH THE RZM OVER THE PHONE. THE RZM WILL SEND A DIGITALLY SIGNED EMAIL CONTAINING THE HASHES TO THE TCR LIST. THE KSR HASHES ARE ALSO SENT TO ICANN BY VERISIGN USING A SECURE WEB SERVICE. THIS DEVIATION FROM THE SCRIPT (ACT 4, STEPS 8, 13, 18 AND 23) IS BEING DOCUMENTED AS AN EXCEPTION.

VERISIGN

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

VerisignInc.com

November 8th, 2018

To Whom It May Concern:

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

Verisign, a global leader in domain names and internet security, enables internet navigation for many of the world's most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key internet infrastructure and services, including the .com and .net top-level domains and two of the internet's root servers, as well as performs the root zone maintainer function for the core of the internet's Domain Name System (DNS). Verisign's Security Services include Distributed Denial of Service Protection and Managed DNS. To learn more about what it means to be Powered by Verisign, visit Verisign.com.

For more than 21 years, the Verisign DNS has maintained 100 percent operational accuracy and stability for .com and .net. Verisign manages and protects the DNS infrastructure for over 149.7 million .com and .net domain names and processes more than 152 billion queries daily-keeping the world connected online, seamlessly and securely. Verisign is experienced in and provides support for both IPv6 and DNSSEC.

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

Sincerely,

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

12061 Bluemont Way,
Reston, VA 20190
t: 703-948-3200

verisign.com

15 November 2018

The SHA256 hash of the 2019 Q1 KSR file is:

ksr-root-2019-q1-0-e_to_f.xml:

d1394356ed2e6b2e496fac97c3ccfe25a5141b2190ad1005ca07 3edc9c3828b9

The PGP wordlist for the hash above is:

PGP Words: stairway corporate crucial escapade tunnel coherence glitter coherence deckhand hemisphere ribcage mosquito snowcap revolver woodlark caravan reindeer belowground beeswax Camelot peachy perceptive assume almighty spellbind Amusement concert sympathy python consulting breadline proximate

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

verisign.com

15 November 2018

The SHA256 hash of the 2019 Q1 KSR file is:

ksr-root-2019-q1-1-f_to_g.xml:

acb4bbf259c993c677c09df5d04ac3ed7e81ce82a3e27c26be75 a07a0e1f94d0

The PGP wordlist for the hash above is:

PGP Words: ribcage politeness shamrock vagabond endow retrospect playhouse responsive involve recipe quadrant visitor stagnate direction snowcap unify locale inventive spyglass Istanbul reform tomorrow kiwi CAretaker skydive impartial ragtime infancy apple businessman Pluto savagery

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

verisign.com

15 November 2018

The SHA256 hash of the 2019 Q1 KSR file is:

ksr-root-2019-q1-2-e_to_e.xml:

32fa1c374e0ba01b4baa62364f3d211d54732640835b220aee04 da0da4e8d255

The PGP wordlist for the hash above is:

PGP Words: checkup whimsical befriend consensus drifter armistice ragtime bravado dragnet pedigree flagpole congregate dropper crucifix blackjack breakaway eating hurricane bookshelf Dakota Mohawk exodus Blockade Apollo tycoon alkali surmount asteroid regain typewriter standard equipment

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

verisign.com

15 November 2018

The SHA256 hash of the 2019 Q1 KSR file is:

ksr-root-2019-q1-3-d_to_d.xml:

12ff64125f43f0ec6994044592b5ce28fdd460452dca9170a9d4 85caec338df3

The PGP wordlist for the hash above is:

PGP Words: atlas Yucatán flytrap backwater eyetooth decimal unearth unicorn gazelle molecule adrift detector physique positive spyglass cellulose willow souvenir facial detector button revenue pheasant hesitate revenge souvenir music revenue tumor concurrent optic vertigo

Attested on behalf of VeriSign by:

Ryan Brown
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

Verify the KSR Hash for Phase E to F

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) IW retains the documents provided by the RZM representative and writes the name: c) RZM representative reads out the PGP word list SHA-256 hash of the KSR file being used.	SR	19:50
9	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	SR	19:50
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/KSK35-0-E_to_F/skr-root-2019-q1-0-e_to_f.xml`**	SR	19:51

Execute the KSR Signer for Phase F to G

Step	Activity	Initials	Time
11	CA executes the command below on the terminal window to sign the KSR file: **`ksrsigner`**[6] **`/media/KSR/KSK35-1-F_to_G/ksr-root-2019-q1-1-f_to_g.xml`**	SR	19:52
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.	SR	19:52

Verify the KSR Hash for Phase F to G

Step	Activity	Initials	Time
13	When the application 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.	SR	19:53
14	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	SR	19:54
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/KSK35-1-F_to_G/skr-root-2019-q1-1-f_to_g.xml`**	SR	19:54

Execute the KSR Signer for Phase E to E

Step	Activity	Initials	Time
16	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[6] `/media/KSR/KSK35-2-E_to_E/ksr-root-2019-q1-2-e_to_e.xml`	SR	19:54
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.	SR	19:55

Verify the KSR Hash for Phase E to E

Step	Activity	Initials	Time
18	When the application 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.	SR	19:56
19	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	SR	19:56
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/KSK35-2-E_to_E/skr-root-2019-q1-2-e_to_e.xml`	SR	19:56

Execute the KSR Signer for Phase D to D

Step	Activity	Initials	Time
21	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[6] `/media/KSR/KSK35-3-D_to_D/ksr-root-2019-q1-3-d_to_d.xml`	SR	19:56
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.	SR	19:57

Verify the KSR Hash for Phase D to D

Step	Activity	Initials	Time
23	When the application 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.	SR	19:58
24	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	SR	19:58
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/KSK35-3-D_to_D/skr-root-2019-q1-3-d_to_d.xml`	SR	19:58

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
26	CA executes the commands below on the terminal window to print the KSR Signer log: a) `lpadmin -p HP -o copies-default=X` **Note: Replace "X" with the amount of copies needed for the participants.** b) `for i in $(ls -1 ksrsigner-20181115*.log); do printlog[7] $i; done`	SR	20:04
27	IW attaches a copy of each ksrsigner log to his/her script.	SR	20:04

Back up the Newly Created SKR

Step	Activity	Initials	Time

28	CA executes the following commands on the terminal window:
	a) List the contents of the KSR FD by executing:
	`ls -ltrR /media/KSR`
	b) Copy the contents of the KSR FD to the HSMFD by executing:
	`cp -pR /media/KSR/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD to verify it has been copied successfully by executing:
	`ls -ltrR`
	d) Flush the system buffers by executing:
	`sync`
	e) unmount the KSR FD by executing:
	`umount /media/KSR`
		SR	20:06

29	CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative.	SR	20:07

```
Starting: ksrsigner /media/KSR/KSK35-0-E_to_F/ksr-root-2019-q1-0-e_to_f.xml (at Thu Nov 15 19:42:36 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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-0-E_to_F/ksr-root-2019-q1-0-e_to_f.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
D1394356ED2E6B2E496FAC97C3CCFE25A5141B2190AD1005CA073EDC9C3828B9
>> stairway corporate crucial escapade tunnel coherence glitter coherence deckhand hemisphere ribcage mosquito snowcap re
volver woodlark caravan reindeer belowground beeswax Camelot peachy perceptive assume almighty spellbind amusement concer
t sympathy python consulting breadline proximate <<

Reading KSK schedule "revoke(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/P,20326(Klajeyz)/S
2 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
3 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
4 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
5 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
6 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
7 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
8 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK35-0-E_to_F/skr-root-2019-q1-0-e_to_f.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/S,19036(Kjqmt7v)/P
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz)/S
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/S

SHA256 hash of SKR:
136B0C39FD0D681CC89D2B01AFF3F8F32056B189332DA0DA59DBD3D1AFEB8B33
>> Aztec Hamilton ammo corporate willow asteroid frighten Brazilian spaniel Ohio briefcase adviser rocker vertigo Vulcan
vertigo bison escapade sailboat matchmaker chisel clergyman ragtime surrender endow suspicious stapler scavenger rocker u
nderfoot obtuse concurrent <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK35-1-F_to_G/ksr-root-2019-q1-1-f_to_g.xml (at Thu Nov 15 19:52:08 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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-1-F_to_G/ksr-root-2019-q1-1-f_to_g.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
ACB4BBF259C993C677C09DF5D04AC3ED7E81CE82A3E27C26BE75A07A0E1F94D0
>> ribcage politeness shamrock vagabond endow retrospect playhouse responsive involve recipe quadrant visitor stagnate di
rection snowcap unify locale inventive spyglass Istanbul reform tomorrow kiwi caretaker skydive impartial ragtime infancy
 apple businessman Pluto savagery <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK35-1-F_to_G/skr-root-2019-q1-1-f_to_g.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/S
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         20326(Klajeyz)/S
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         20326(Klajeyz)/S
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         20326(Klajeyz)/S
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         20326(Klajeyz)/S
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         20326(Klajeyz)/S
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         20326(Klajeyz)/S
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         20326(Klajeyz)/S
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/S

SHA256 hash of SKR:
6FFF311585EF2DA8E925D92599070BCA2ACCBABB62D6740D09299DE3A77C6E7A
>> gremlin Yucatan chatter bifocals music unravel button paramount treadmill caravan sugar caravan prowler amusement alon
e revenue brickyard revolver shadow publisher flagpole speculate indoors asteroid Algol certify quadrant torpedo repay in
formant goldfish infancy <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK35-2-E_to_E/ksr-root-2019-q1-2-e_to_e.xml (at Thu Nov 15 19:54:48 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:         H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-2-E_to_E/ksr-root-2019-q1-2-e_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
32FA1C374E0BA01B4BAA62364F3D211D54732640835B220AEE04DA0DA4E8D255
>> checkup whimsical befriend consensus drifter armistice ragtime bravado dragnet pedigree flagpole congregate dropper cr
ucifix blackjack breakaway eating hurricane bookshelf Dakota Mohawk exodus blockade Apollo tycoon alkali surmount asteroi
d regain typewriter standard equipment <<

Reading KSK schedule "rollover+(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/P,20326(Klajeyz)/S
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/KSK35-2-E_to_E/skr-root-2019-q1-2-e_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/S,19036(Kjqmt7v)/P
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/S,19036(Kjqmt7v)/P

SHA256 hash of SKR:
3B831414061BA7CA4FE016A04334DF7030394FF30E0B218D95D012C1D70A8513
>> clockwork Jamaica baboon belowground afflict bravado repay revenue dropper tobacco backward Orlando crucial confidence
 talon hesitate chairlift corporate dropper vertigo apple armistice blackjack microscope preclude savagery atlas recover
stopwatch Apollo music barbecue <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK35-3-D_to_D/ksr-root-2019-q1-3-d_to_d.xml (at Thu Nov 15 19:56:52 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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-3-D_to_D/ksr-root-2019-q1-3-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
12FF64125F43F0EC6994044592B5CE28FDD460452DCA9170A9D485CAEC338DF3
>> atlas Yucatan flytrap backwater eyetooth decimal unearth unicorn gazelle molecule adrift detector physique positive sp
yglass cellulose willow souvenir facial detector button revenue pheasant hesitate revenge souvenir music revenue tumor co
ncurrent optic vertigo <<

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/KSK35-3-D_to_D/skr-root-2019-q1-3-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
99DF85FBDF5F480F549F60A9355587B8E84E704EED906451642FA9B74301F7EC
>> prowler therapist music Wichita talon forever deadbolt atmosphere eating opulent facial passenger chopper equipment Ne
ptune provincial trauma distortion guidance distortion tunnel millionaire flytrap enchanting flytrap combustion revenge p
rocessor crucial adviser virus unicorn <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

Disable/Deactivate the HSM

Step	Activity	Initials	Time
30	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 5 of 7 2nd OP card 6 of 7 3rd OP card 4 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	SK	20:11

Act 5. Secure Hardware

The CA backs up the HSMDF flash drive contents, prints log information and place the equipment and the TCRs cards inside of Tamper Evident Bags. Then the CA and IW escort the SSCs and TCRs into the Tier 5 (safe room) to return the equipment to Safe 1 and the TCRs cards to Safe 2.

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.**	SR	20:11
2	CA places the HSM into a prepared TEB, then seals it.	SR	20:13
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. **HSM4: TEB # BB51184680 / Serial # H1411011**	SR	20:14

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)**: i) Press `Ctrl + C` ii) 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.**	SR	20:15

Back up the HSMFD Contents

Step	Activity	Initials	Time
5	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: `shopt -s dotglob`	SR	20:16
6	CA executes the following commands on the terminal window to print 2 copies of the hash for the HSMFD content: a) `lpadmin -p HP -o copies-default=2` b) `hsmfd-hash[3] -p` **Note: One copy for audit bundle and one copy for HSMFD package.**	SR	20:18
7	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrR`	SR	20:18
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**	SR	20:19
9	CA closes the file system window, then executes the command below to back up the HSMFD: `cp -pR * /media/HSMFD1`	SR	20:19
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[3] -m`	SR	20:20
11	CA executes the command below using the terminal window to unmount the HSMFD copy: `umount /media/HSMFD1`	SR	20:20
12	CA removes the **HSMFD1**, then places it on the holder.	SR	20:21
13	CA repeats step 8 to 12 for the 2nd copy.	SR	20:22
14	CA repeats step 8 to 12 for the 3rd copy.	SR	20:22
15	CA repeats step 8 to 12 for the 4th copy.	SR	20:23
16	CA repeats step 8 to 12 for the 5th copy.	SR	20:24

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: a) `lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true` b) `enscript -2Gr script-201811*.log` c) `enscript -Gr --font="Courier8" ttyaudit-tty*-201811*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**	SR	20:28

HSMFD SHA-256 HASH **2018/11/15**

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

SHA-256:    6763b5009de602ddd81797839410ffe223273947193f1ff3d35f4583d3dfaf11
PGP Words:  freedom Galveston scorecard adroitness quadrant trombonist accrue tambourine st
ormy bookseller preshrunk Jamaica Pluto autopsy Zulu tomorrow blowtorch celebrate classroom
 determine bedlamp customer billiard vertigo stapler forever crusade Jamaica stapler therap
ist rocker Babylon
```

```
Script started on Thu Nov 15 19:27:14 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=0.988 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.571 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.742 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.577 ms
64 bytes from hsm (192.168.0.2): icmp_seq=5 ttl=255 time=0.576 ms
64 bytes from hsm (192.168.0.2): icmp_seq=6 ttl=255 time=0.576 ms
64 bytes from hsm (192.168.0.2): icmp_seq=7 ttl=255 time=0.571 ms
^C
--- hsm ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6123ms
rtt min/avg/max/mdev = 0.571/0.657/0.988/0.148 ms
root@coen:/media/HSMFD# ksrsigner /media/KSR/KSK\00735-0-E_to_F/ks\007r-root-2019-q1-0-e_
to_f.xml
Starting: ksrsigner /media/KSR/KSK35-0-E_to_F/ksr-root-2019-q1-0-e_to_f.xml (at Thu Nov 1
5 19:42:36 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_glib
c_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.s
o.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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-0-E_to_F/ksr-root-2019-q1-0-e_to_f.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
D1394356ED2E6B2E496FAC97C3CCFE25A5141B2190AD1005CA073EDC9C3828B9
>> stairway corporate crucial escapade tunnel coherence glitter coherence deckhand hemisp
here ribcage mosquito snowcap revolver woodlark caravan reindeer belowground beeswax Came
lot peachy perceptive assume almighty spellbind amusement concert sympathy python consult
ing breadline proximate <<
Is this correct (y/N)? y

Reading KSK schedule "revoke(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/P,20326(Klajeyz)/S
2 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
3 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
4 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
5 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
6 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
7 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
8 20326(Klajeyz)/S,19164(Kjqmt7v)/RS
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK35-0-E_to_F/skr-root-2019-q1-0-e_to_f.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/S,19036(Kjqmt7v)
/P
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         19164(Kjqmt7v)/RS,20326(Klajeyz
)/S
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/S

SHA256 hash of SKR:
136B0C39FD0D681CC89D2B01AFF3F8F32056B189332DA0DA59DBD3D1AFEB8B33
>> Aztec Hamilton ammo corporate willow asteroid frighten Brazilian spaniel Ohio briefcas
e adviser rocker vertigo Vulcan vertigo bison escapade sailboat matchmaker chisel clergym
an ragtime surrender endow suspicious stapler scavenger rocker underfoot obtuse concurren
t <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20181115-194236.log **********
root@coen:/media/HSMFD# ksrsign
root@coen:/media/HSMFD# ksrsigner /media/KSR/KSK\00735-1-F_to_G/ksr-root-2019-q1-1-f_to_g
.xml
Starting: ksrsigner /media/KSR/KSK35-1-F_to_G/ksr-root-2019-q1-1-f_to_g.xml (at Thu Nov 1
5 19:52:08 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_glib
c_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.s
o.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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-1-F_to_G/ksr-root-2019-q1-1-f_to_g.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
ACB4BBF259C993C677C09DF5D04AC3ED7E81CE82A3E27C26BE75A07A0E1F94D0
>> ribcage politeness shamrock vagabond endow retrospect playhouse responsive involve rec
ipe quadrant visitor stagnate direction snowcap unify locale inventive spyglass Istanbul
reform tomorrow kiwi caretaker skydive impartial ragtime infancy apple businessman Pluto
savagery <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK35-1-F_to_G/skr-root-2019-q1-1-f_to_g.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/S
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         20326(Klajeyz)/S
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         20326(Klajeyz)/S
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         20326(Klajeyz)/S
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         20326(Klajeyz)/S
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         20326(Klajeyz)/S
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         20326(Klajeyz)/S
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         20326(Klajeyz)/S
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/S

SHA256 hash of SKR:
6FFF311585EF2DA8E925D92599070BCA2ACCBABB62D6740D09299DE3A77C6E7A
>> gremlin Yucatan chatter bifocals music unravel button paramount treadmill caravan suga
r caravan prowler amusement alone revenue brickyard revolver shadow publisher flagpole sp
eculate indoors asteroid Algol certify quadrant torpedo repay informant goldfish infancy
<<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20181115-195208.log **********
root@coen:/media/HSMFD#
root@coen:/media/HSMFD# ksrsigner /media/KSR/KSK\00735-2-E_to_E/ksr-root-2019-q1-2-e_to_e
.xml
Starting: ksrsigner /media/KSR/KSK35-2-E_to_E/ksr-root-2019-q1-2-e_to_e.xml (at Thu Nov 1
5 19:54:48 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_glib
c_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.s
o.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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-2-E_to_E/ksr-root-2019-q1-2-e_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
32FA1C374E0BA01B4BAA62364F3D211D54732640835B220AEE04DA0DA4E8D255
>> checkup whimsical befriend consensus drifter armistice ragtime bravado dragnet pedigre
e flagpole congregate dropper crucifix blackjack breakaway eating hurricane bookshelf Dak
ota Mohawk exodus blockade Apollo tycoon alkali surmount asteroid regain typewriter stand
ard equipment <<
Is this correct (y/N)? y

Reading KSK schedule "rollover+(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/P,20326(Klajeyz)/S
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/KSK35-2-E_to_E/skr-root-2019-q1-2-e_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/S,19036(Kjqmt7v)
/P
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         20326(Klajeyz)/S,19036(Kjqmt7v)
/P
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/S,19036(Kjqmt7v)
/P

SHA256 hash of SKR:
3B831414061BA7CA4FE016A04334DF7030394FF30E0B218D95D012C1D70A8513
>> clockwork Jamaica baboon belowground afflict bravado repay revenue dropper tobacco bac
kward Orlando crucial confidence talon hesitate chairlift corporate dropper vertigo apple
 armistice blackjack microscope preclude savagery atlas recover stopwatch Apollo music ba
rbecue <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20181115-195448.log **********
root@coen:/media/HSMFD#
root@coen:/media/HSMFD# ksrsigner /media/KSR/KSK\00735-3-D_to_D/ksr-root-2019-q1-3-d_to_d
.xml
Starting: ksrsigner /media/KSR/KSK35-3-D_to_D/ksr-root-2019-q1-3-d_to_d.xml (at Thu Nov 1
5 19:56:52 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_glib
c_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.s
o.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:          H1411011

Validating last SKR with HSM...
#  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
...VALIDATED.

Validate and Process KSR /media/KSR/KSK35-3-D_to_D/ksr-root-2019-q1-3-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  16749,02134
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749
9  2019-03-22T00:00:00 2019-04-12T00:00:00  16749,25266
...PASSED.

SHA256 hash of KSR:
12FF64125F43F0EC6994044592B5CE28FDD460452DCA9170A9D485CAEC338DF3
>> atlas Yucatan flytrap backwater eyetooth decimal unearth unicorn gazelle molecule adri
```

```
ft detector physique positive spyglass cellulose willow souvenir facial detector button r
evenue pheasant hesitate revenge souvenir music revenue tumor concurrent optic vertigo <<
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/KSK35-3-D_to_D/skr-root-2019-q1-3-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2019-01-01T00:00:00 2019-01-22T00:00:00  02134,16749   20326(Klajeyz)/P,19036(Kjqmt7v)
/S
2  2019-01-11T00:00:00 2019-02-01T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
3  2019-01-21T00:00:00 2019-02-11T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
4  2019-01-31T00:00:00 2019-02-21T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
5  2019-02-10T00:00:00 2019-03-03T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
6  2019-02-20T00:00:00 2019-03-13T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
7  2019-03-02T00:00:00 2019-03-23T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
8  2019-03-12T00:00:00 2019-04-02T00:00:00  16749         20326(Klajeyz)/P,19036(Kjqmt7v)
/S
9  2019-03-22T00:00:00 2019-04-12T00:00:00  25266,16749   20326(Klajeyz)/P,19036(Kjqmt7v)
/S

SHA256 hash of SKR:
99DF85FBDF5F480F549F60A9355587B8E84E704EED906451642FA9B74301F7EC
>> prowler therapist music Wichita talon forever deadbolt atmosphere eating opulent facia
l passenger chopper equipment Neptune provincial trauma distortion guidance distortion tu
nnel millionaire flytrap enchanting flytrap combustion revenge processor crucial adviser
virus unicorn <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20181115-195652.log **********
root@coen:/media/HSMFD#
root@coen:/media/HSMFD# lpadmin -p HP -o copies-default=6
root@coen:/media/HSMFD# for i in $(ls -1 ksr\007signer-20181115*.log); do printlog $i; do
ne
[ 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# ls -ltrR /media/KSR/
/media/KSR/:
total 16
drwxr-xr-x 2 root root 4096 Nov 15 19:50 \033[0m\033[01;34mKSK35-0-E_to_F\033[0m
drwxr-xr-x 2 root root 4096 Nov 15 19:54 \033[01;34mKSK35-1-F_to_G\033[0m
drwxr-xr-x 2 root root 4096 Nov 15 19:56 \033[01;34mKSK35-2-E_to_E\033[0m
drwxr-xr-x 2 root root 4096 Nov 15 19:58 \033[01;34mKSK35-3-D_to_D\033[0m

/media/KSR/KSK35-0-E_to_F:
total 116
-rw-r--r-- 1 root root  1678 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-0-e_to_f.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115194236
-rw-r--r-- 1 root root 29640 Nov 15 19:50 skr.xml
-rw-r--r-- 1 root root 29640 Nov 15 19:50 skr-root-2019-q1-0-e_to_f.xml

/media/KSR/KSK35-1-F_to_G:
total 92
-rw-r--r-- 1 root root  1148 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-1-f_to_g.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115195208
-rw-r--r-- 1 root root 20367 Nov 15 19:54 skr.xml
-rw-r--r-- 1 root root 20367 Nov 15 19:54 skr-root-2019-q1-1-f_to_g.xml

/media/KSR/KSK35-2-E_to_E:
total 108
-rw-r--r-- 1 root root  1345 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-2-e_to_e.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115195448
-rw-r--r-- 1 root root 24948 Nov 15 19:56 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15 19:56 skr-root-2019-q1-2-e_to_e.xml

/media/KSR/KSK35-3-D_to_D:
total 108
-rw-r--r-- 1 root root  1344 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-3-d_to_d.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115195652
-rw-r--r-- 1 root root 24948 Nov 15 19:58 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15 19:58 skr-root-2019-q1-3-d_to_d.xml
root@coen:/media/HSMFD# cp -pR /media/KSR/* .
root@coen:/media/HSMFD# ls -ltrR
.:
total 2164
-rw-r--r-- 1 root root  15547 Jun  9  2010 ksr-root-2010-q3-2.xml
-rw-r--r-- 1 root root  40555 Jun  9  2010 wksr-20100517-172720.log
-rw-r--r-- 1 root root    190 Jun 16  2010 KSKSlotDB.config.db
-rw-r--r-- 1 root root   2668 Jun 16  2010 kskgen-20100616-211906.log
-rw-r--r-- 1 root root    765 Jun 16  2010 Kjqmt7v.csr
-rw-r--r-- 1 root root  36864 Jun 16  2010 ttyaudit-ttyUSB1-20100616-182157.log
-rw-r--r-- 1 root root  45056 Jun 16  2010 ttyaudit-ttyUSB0-20100616-182157.log
-rw-r--r-- 1 root root  18364 Jun 16  2010 skr-root-2010-q3-2.xml
-rw-r--r-- 1 root root   4473 Jun 16  2010 ksrsigner-20100616-214329.log
-rw-r--r-- 1 root root 196608 Jun 16  2010 script-20100616.log
-rw-r--r-- 1 root root   7674 Jun 16  2010 script-20100616-2209utc.log
-rw-r--r-- 1 root root  18364 Oct 31  2010 skr.xml.20101101181303
-rw-r--r-- 1 root root  15547 Oct 31  2010 ksr-root-2011-q1-0.xml
-rw-r--r-- 1 root root  18402 Nov  1  2010 skr-root-2011-q1-0.xml
-rw-r--r-- 1 root root   5504 Nov  1  2010 ksrsigner-20101101-181303.log
-rw-r--r-- 1 root root  14005 Nov  1  2010 ttyaudit-ttyUSB0-20101101-175457.log
-rw-r--r-- 1 root root   7161 Nov  1  2010 script-20101101.log
-rw-r--r-- 1 root root  18402 Feb  7  2011 skr.xml.20110511181632
-rw-r--r-- 1 root root  15547 Apr 25  2011 ksr-root-2011-q3-0.xml
-rw-r--r-- 1 root root   1400 May 11  2011 ksrsigner-20110511-181351.log
-rw-r--r-- 1 root root  18402 May 11  2011 skr-root-2011-q3-0.xml
-rw-r--r-- 1 root root   5510 May 11  2011 ksrsigner-20110511-181632.log
-rw-r--r-- 1 root root  14374 May 11  2011 ttyaudit-ttyUSB0-20110511-180559.log
-rw-r--r-- 1 root root   9133 May 11  2011 script-20110511.log
-rw-r--r-- 1 root root  18404 Jul 20  2011 skr.xml.20110930181607
-rw-r--r-- 1 root root  15587 Sep 23  2011 ksr-root-2012-q1-0.xml
-rw-r--r-- 1 root root  18422 Sep 30  2011 skr-root-2012-q1-0.xml
```

```
-rw-r--r-- 1 root root   5609 Sep 30  2011 ksrsigner-20110930-181607.log
-rw-r--r-- 1 root root  12034 Sep 30  2011 ttyaudit-ttyUSB0-20110930-180703.log
-rw-r--r-- 1 root root   7270 Sep 30  2011 script-20110930.log
-rw-r--r-- 1 root root  18424 Feb  2  2012 skr.xml.20120522151741
-rw-r--r-- 1 root root  15571 May  9  2012 ksr-root-2012-q3-0.xml
-rw-r--r-- 1 root root  18414 May 22  2012 skr-root-2012-q3-0.xml
-rw-r--r-- 1 root root   5528 May 22  2012 ksrsigner-20120522-151741.log
-rw-r--r-- 1 root root  12034 May 22  2012 ttyaudit-ttyUSB0-20120522-150621.log
-rw-r--r-- 1 root root  13817 May 22  2012 script-20120522.log
-rw-r--r-- 1 root root  18324 Jul 26  2012 skr.xml.20121112155152
-rw-r--r-- 1 root root  15371 Oct 12  2012 ksr-root-2013-q1-0.xml
-rw-r--r-- 1 root root  18314 Nov 12  2012 skr-root-2013-q1-0.xml
-rw-r--r-- 1 root root   5529 Nov 12  2012 ksrsigner-20121112-155152.log
-rw-r--r-- 1 root root  12044 Nov 12  2012 ttyaudit-ttyUSB0-20121112-154229.log
-rw-r--r-- 1 root root  12249 Nov 12  2012 script-20121112.log
-rw-r--r-- 1 root root  18314 Feb 12  2013 skr.xml.20130502190633
-rw-r--r-- 1 root root  15371 Apr  5  2013 ksr-root-2013-q3-0.xml
-rw-r--r-- 1 root root   4004 May  2  2013 ksrsigner-20130502-190252.log
-rw-r--r-- 1 root root  18314 May  2  2013 skr-root-2013-q3-0.xml
-rw-r--r-- 1 root root   5502 May  2  2013 ksrsigner-20130502-190633.log
-rw-r--r-- 1 root root  12397 May  2  2013 ttyaudit-ttyUSB0-20130502-185222.log
-rw-r--r-- 1 root root  21494 May  2  2013 script-20130502.log
-rw-r--r-- 1 root root  18314 Aug  7  2013 skr.xml.20131024184618
-rw-r--r-- 1 root root  15371 Oct  4  2013 ksr-root-2014-q1-0.xml
-rw-r--r-- 1 root root  18314 Oct 24  2013 skr-root-2014-q1-0.xml
-rw-r--r-- 1 root root   5512 Oct 24  2013 ksrsigner-20131024-184618.log
-rw-r--r-- 1 root root  12044 Oct 24  2013 ttyaudit-ttyUSB0-20131024-182843.log
-rw-r--r-- 1 root root   9167 Oct 24  2013 script-20131024.log
-rw-r--r-- 1 root root  18314 Feb 13  2014 skr.xml.20140417183604
-rw-r--r-- 1 root root  15353 Apr  3  2014 ksr-root-2014-q3-0.xml
-rw-r--r-- 1 root root  18314 Apr 17  2014 skr-root-2014-q3-0.xml
-rw-r--r-- 1 root root   5511 Apr 17  2014 ksrsigner-20140417-183604.log
-rw-r--r-- 1 root root  12034 Apr 17  2014 ttyaudit-ttyUSB0-20140417-182117.log
-rw-r--r-- 1 root root   5853 Apr 17  2014 script-20140417.log
-rw-r--r-- 1 root root  18314 Nov 10  2014 skr.xml.20141120201132
-rw-r--r-- 1 root root  15371 Nov 10  2014 ksr-root-2015-q1-0.xml
-rw-r--r-- 1 root root  18314 Nov 20  2014 skr-root-2015-q1-0.xml
-rw-r--r-- 1 root root   5490 Nov 20  2014 ksrsigner-20141120-201132.log
-rw-r--r-- 1 root root  12042 Nov 20  2014 ttyaudit-ttyUSB0-20141120-200407.log
-rw-r--r-- 1 root root   5462 Nov 20  2014 script-20141120-1.log
-rw-r--r-- 1 root root  15353 Apr  1  2015 ksr-root-2015-q3-0.xml
-rw-r--r-- 1 root root  18314 Apr  1  2015 skr.xml.20150409183038
-rw-r--r-- 1 root root  18314 Apr  9  2015 skr-root-2015-q3-0.xml
-rw-r--r-- 1 root root   5621 Apr  9  2015 ksrsigner-20150409-183038.log
-rw-r--r-- 1 root root  15774 Apr  9  2015 ttyaudit-ttyUSB0-20150409-180743.log
-rw-r--r-- 1 root root   5636 Apr  9  2015 ksrsigner-20150409-193635.log
-rw-r--r-- 1 root root  33966 Apr  9  2015 ttyaudit-ttyUSB0-20150409-190117.log
-rw-r--r-- 1 root root   5636 Apr  9  2015 ksrsigner-20150409-205227.log
-rw-r--r-- 1 root root  34895 Apr  9  2015 ttyaudit-ttyUSB0-20150409-202837.log
-rw-r--r-- 1 root root  19175 Apr  9  2015 script-20150409.log
-rw-r--r-- 1 root root  18314 Nov  4  2015 skr.xml.20151112193232
-rw-r--r-- 1 root root  15371 Nov  4  2015 ksr-root-2016-q1-0.xml
-rw-r--r-- 1 root root  18314 Nov 12  2015 skr-root-2016-q1-0.xml
-rw-r--r-- 1 root root   5547 Nov 12  2015 ksrsigner-20151112-193232.log
-rw-r--r-- 1 root root  12215 Nov 12  2015 ttyaudit-ttyUSB0-20151112-191111.log
-rw-r--r-- 1 root root   7282 Nov 12  2015 script-20151112.log
-rw-r--r-- 1 root root  18314 Apr 29  2016 skr.xml.20160512192325
-rw-r--r-- 1 root root  14301 Apr 29  2016 ksr-root-2016-q3-fallback-1.xml
-rw-r--r-- 1 root root  18314 Apr 29  2016 skr.xml.20160512190619
-rw-r--r-- 1 root root  15994 Apr 29  2016 ksr-root-2016-q3-0.xml
-rw-r--r-- 1 root root  18599 May 12  2016 skr-root-2016-q3-0.xml
-rw-r--r-- 1 root root   5534 May 12  2016 ksrsigner-20160512-190619.log
-rw-r--r-- 1 root root  17908 May 12  2016 skr-root-2016-q3-fallback-1.xml
-rw-r--r-- 1 root root   5566 May 12  2016 ksrsigner-20160512-192325.log
-rw-r--r-- 1 root root  12484 May 12  2016 ttyaudit-ttyUSB0-20160512-184752.log
-rw-r--r-- 1 root root  15870 May 12  2016 script-20160512.log
-rw-r--r-- 1 root root  19557 Oct 24  2016 ksr-root-2017-q1-0.xml
-rw-r--r-- 1 root root  21083 Oct 24  2016 skr.xml.20161027183803
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr.xml
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr-root-2017-q1-0.xml
-rw-r--r-- 1 root root   5501 Oct 27  2016 ksrsigner-20161027-183803.log
-rw-r--r-- 1 root root   2712 Oct 27  2016 kskgen-20161027-184920.log
-rw-r--r-- 1 root root    817 Oct 27  2016 Klajeyz.csr
-rw-r--r-- 1 root root   2974 Oct 27  2016 KSKSlotDB.db
-rw-r--r-- 1 root root    357 Oct 27  2016 keybackup-20161027-185705.log
-rw-r--r-- 1 root root    357 Oct 27  2016 keybackup-20161027-200501.log
-rw-r--r-- 1 root root  28791 Oct 27  2016 ttyaudit-ttyUSB0-20161027-182428.log
-rw-r--r-- 1 root root  33568 Oct 27  2016 ttyaudit-ttyUSB0-20161027-202240.log
-rw-r--r-- 1 root root  17803 Oct 27  2016 script-20161027.log
-rw-r--r-- 1 root root   6505 Apr 27  2017 ksrsigner-20170427-183853.log
drwxr-xr-x 2 root root   4096 Apr 27  2017 \033[0m\033[01;34mKSK29-0-C_to_D\033[0m
-rw-r--r-- 1 root root   6228 Apr 27  2017 ksrsigner-20170427-184519.log
drwxr-xr-x 2 root root   4096 Apr 27  2017 \033[01;34mKSK29-1-D_to_C\033[0m
-rw-r--r-- 1 root root   6224 Apr 27  2017 ksrsigner-20170427-184912.log
drwxr-xr-x 2 root root   4096 Apr 27  2017 \033[01;34mKSK29-2-C_to_C\033[0m
-rw-r--r-- 1 root root  12913 Apr 27  2017 ttyaudit-ttyUSB0-20170427-182024.log
-rw-r--r-- 1 root root  16683 Apr 27  2017 script-20170427.log
-rw-r--r-- 1 root root      0 Oct 18  2017 script-20171018.log
-rw-r--r-- 1 root root   8192 Oct 18  2017 ttyaudit-ttyUSB0-20171018-174745.log
-rw-r--r-- 1 root root   6681 Oct 18  2017 ksrsigner-20171018-181941.log
drwxr-xr-x 2 root root   4096 Oct 18  2017 \033[01;34mKSK31-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6698 Oct 18  2017 ksrsigner-20171018-182803.log
drwxr-xr-x 2 root root   4096 Oct 18  2017 \033[01;34mKSK31-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6678 Oct 18  2017 ksrsigner-20171018-183150.log
drwxr-xr-x 2 root root   4096 Oct 18  2017 \033[01;34mKSK31-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6361 Oct 18  2017 ksrsigner-20171018-183453.log
drwxr-xr-x 2 root root   4096 Oct 18  2017 \033[01;34mKSK31-3-C_to_C\033[0m
-rw-r--r-- 1 root root   4384 Oct 18  2017 ttyaudit-ttyUSB0-20171018-175253.log
-rw-r--r-- 1 root root  23163 Oct 18  2017 script-20171018-v2.log
-rw-r--r-- 1 root root  10002 Apr 11  2018 ttyaudit-ttyUSB0-20180411-181102.log
-rw-r--r-- 1 root root   6775 Apr 11  2018 ksrsigner-20180411-183203.log
drwxr-xr-x 2 root root   4096 Apr 11  2018 \033[01;34mKSK33-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6783 Apr 11  2018 ksrsigner-20180411-183607.log
drwxr-xr-x 2 root root   4096 Apr 11  2018 \033[01;34mKSK33-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6776 Apr 11  2018 ksrsigner-20180411-183814.log
drwxr-xr-x 2 root root   4096 Apr 11  2018 \033[01;34mKSK33-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6469 Apr 11  2018 ksrsigner-20180411-184001.log
drwxr-xr-x 2 root root   4096 Apr 11  2018 \033[01;34mKSK33-3-C_to_C\033[0m
-rw-r--r-- 1 root root      0 Apr 11  2018 ttyaudit-ttyUSB0-20180411-185854.log
-rw-r--r-- 1 root root  36029 Apr 11  2018 script-20180411.log
-rw-r--r-- 1 root root   6757 Nov 15 19:50 ksrsigner-20181115-194236.log
drwxr-xr-x 2 root root   4096 Nov 15 19:50 \033[01;34mKSK35-0-E_to_F\033[0m
-rw-r--r-- 1 root root   6449 Nov 15 19:54 ksrsigner-20181115-195208.log
drwxr-xr-x 2 root root   4096 Nov 15 19:54 \033[01;34mKSK35-1-F_to_G\033[0m
-rw-r--r-- 1 root root   6775 Nov 15 19:56 ksrsigner-20181115-195448.log
drwxr-xr-x 2 root root   4096 Nov 15 19:56 \033[01;34mKSK35-2-E_to_E\033[0m
-rw-r--r-- 1 root root  13534 Nov 15 19:58 ttyaudit-ttyS0-20181115-192849.log
drwxr-xr-x 2 root root   4096 Nov 15 19:58 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root  20480 Nov 15 19:58 script-20181115.log
-rw-r--r-- 1 root root   6765 Nov 15 19:58 ksrsigner-20181115-195652.log
drwxr-xr-x 2 root root   4096 Nov 15 19:58 \033[01;34mKSK35-3-D_to_D\033[0m

./KSK29-0-C_to_D:
total 92
-rw-r--r-- 1 root root 20347 Apr 20  2017 skr.xml.20170427183853
-rw-r--r-- 1 root root 19556 Apr 20  2017 ksr-root-2017-q3-0-c_to_d.xml
-rw-r--r-- 1 root root   540 Apr 20  2017 kskschedule.json
-rw-r--r-- 1 root root 24419 Apr 27  2017 skr.xml
```

```
-rw-r--r-- 1 root root 24419 Apr 27  2017 skr-root-2017-q3-0-c_to_d.xml

./KSK29-1-D_to_C:
total 84
-rw-r--r-- 1 root root 20347 Apr 20  2017 skr.xml.20170427184519
-rw-r--r-- 1 root root 19556 Apr 20  2017 ksr-root-2017-q3-1-d_to_c.xml
-rw-r--r-- 1 root root   454 Apr 20  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr.xml
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr-root-2017-q3-1-d_to_c.xml

./KSK29-2-C_to_C:
total 84
-rw-r--r-- 1 root root 20347 Apr 20  2017 skr.xml.20170427184912
-rw-r--r-- 1 root root 19556 Apr 20  2017 ksr-root-2017-q3-2-c_to_c.xml
-rw-r--r-- 1 root root   454 Apr 20  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr.xml
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr-root-2017-q3-2-c_to_c.xml

./KSK31-0-D_to_E:
total 108
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018181941
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-0-d_to_e.xml

./KSK31-1-E_to_D:
total 108
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018182803
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-1-e_to_d.xml

./KSK31-2-D_to_D:
total 108
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018183150
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-2-d_to_d.xml

./KSK31-3-C_to_C:
total 92
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018183453
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 20347 Oct 18  2017 skr-root-2018-q1-3-c_to_c.xml

./KSK33-0-D_to_E:
total 108
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411183203
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr-root-2018-q3-0-d_to_e.xml

./KSK33-1-E_to_D:
total 108
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411183607
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr-root-2018-q3-1-e_to_d.xml

./KSK33-2-D_to_D:
total 108
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411183814
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr-root-2018-q3-2-d_to_d.xml

./KSK33-3-C_to_C:
total 92
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411184001
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 20347 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 20347 Apr 11  2018 skr-root-2018-q3-3-c_to_c.xml

./KSK35-0-E_to_F:
total 116
-rw-r--r-- 1 root root  1678 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-0-e_to_f.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115194236
-rw-r--r-- 1 root root 29640 Nov 15 19:50 skr.xml
-rw-r--r-- 1 root root 29640 Nov 15 19:50 skr-root-2019-q1-0-e_to_f.xml

./KSK35-1-F_to_G:
total 92
-rw-r--r-- 1 root root  1148 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-1-f_to_g.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115195208
-rw-r--r-- 1 root root 20367 Nov 15 19:54 skr.xml
-rw-r--r-- 1 root root 20367 Nov 15 19:54 skr-root-2019-q1-1-f_to_g.xml

./KSK35-2-E_to_E:
total 108
-rw-r--r-- 1 root root  1345 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-2-e_to_e.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115195448
-rw-r--r-- 1 root root 24948 Nov 15 19:56 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15 19:56 skr-root-2019-q1-2-e_to_e.xml

./tmp:
total 40
-rw-r--r-- 1 root root  880 May  2  2013 ksrsigner_20130502190252_5048_tmp_skr.xml
-rw-r--r-- 1 root root 2144 Nov 15 19:58 skr.keybundle.8
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.7
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.6
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.5
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.4
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.3
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.2
-rw-r--r-- 1 root root 1768 Nov 15 19:58 skr.keybundle.1
-rw-r--r-- 1 root root 2144 Nov 15 19:58 skr.keybundle.0

./KSK35-3-D_to_D:
total 108
-rw-r--r-- 1 root root  1344 Oct 12 15:10 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9 09:17 ksr-root-2019-q1-3-d_to_d.xml
-rw-r--r-- 1 root root 24930 Nov  9 09:33 skr.xml.20181115195652
-rw-r--r-- 1 root root 24948 Nov 15 19:58 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15 19:58 skr-root-2019-q1-3-d_to_d.xml
root@coen:/media/HSMFD# sync
root@coen:/media/HSMFD# umount /media/KSR/
```

```
k088[Kroot@media/HSMFD#HSMFD# exit
exit

Script done on Thu Nov 15 20:15:50 2018
```

```
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0	H1411011 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0	BBL CRC32: 0x757574CA
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0	Running applicationBootLoader at 0xEFDC0000
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0	H1411011 011403 ABL 011 : Tamper Challenge Response Key
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:57+0000	ttyS0	ABL CRC32: 0xE7E0FA6A
2018-11-15T19:29:57+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	####################################
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	###     ABL tamper records       ###
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	####################################
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	Current Tamper Counts (decimal 0-255):
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	====================================
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	vextoosTamperCount:     0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	vintoosTamperCount:     15
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	vbboosTamperCount:      0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	maxstrtempTamperCount:  0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	minstrtempTamperCount:  0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	meshTamperCount:        0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	extampSMKTamperCount:   0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	extampIMKTamperCount:   0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	tempdiffTamperCount:    0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	pfTamperCount:          15
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	restartTamperCount:     31
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	Current tamper bitmaps:
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	======================
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	currentTamper bitmap:   0x0000 0b .... .... .... ....
2018-11-15T19:29:58+0000	ttyS0
2018-11-15T19:29:58+0000	ttyS0	lastTamper bitmap:      0x0000 0b .... .... .... ....
```

```
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:58+0000        ttyS0   Bitmapped Change Record (most recent first):
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:58+0000        ttyS0   ========================================
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:58+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Running cryptoApplication at 0xEBF00000
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Jumping to startup @ 0x001037B4
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Board is P2020RDB
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   board_smp_init: 2 cpu
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Starting next program at v0015183c
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Starting K-Series Kernel
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Copyright AEP Networks Ltd. All Rights Reserved.
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:29:59+0000        ttyS0   Thu Nov 15 18:22:04 2018
2018-11-15T19:29:59+0000        ttyS0
2018-11-15T19:30:00+0000        ttyS0   Starting auditd v2.0 ... started.
2018-11-15T19:30:00+0000        ttyS0
2018-11-15T19:30:00+0000        ttyS0   Interface 0 configured for IPv6.
2018-11-15T19:30:00+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   Interface 0 configured for IPv4.
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   route: writing to routing socket: Network is unreachable
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   add net default: gateway ::: Network is unreachable
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   route: writing to routing socket: Network is unreachable
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   Starting USB driver...
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0   9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:01+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running DES POST Test
2018-11-15T19:30:03+0000        ttyS0
```

```
2018-11-15T19:30:03+0000        ttyS0   DES POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running Triple DES POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Triple DES POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running AES POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   AES POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running SHA1 POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   SHA1 POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running SHA2 POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   SHA2 POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running RandomGen POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   RandomGen POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running RSA POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   RSA POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running DSA POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   DSA POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   Running ECC POST Test
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:03+0000        ttyS0   ECC POST Test Passed
2018-11-15T19:30:03+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0   Audit on 15/11/2018 18:22:07 00100008
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0   Keyper 9860-2  Serial Number H1411011
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0   Memory Usage:
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0   RAM (free/total)        197Mb/256Mb
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0   Flash (free/total)      127Mb/128Mb
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0      black store          512b
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0      statistics           112b
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0      other                116b
2018-11-15T19:30:04+0000        ttyS0
2018-11-15T19:30:04+0000        ttyS0   RedStore (free/total)   109Kb/128Kb
```

```
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	Network Configuration:
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	IPv4: enabled
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	IPv6: enabled
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	MAC/IP address(es): 00:E0:06:C0:B3:2A / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b32a/64
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	HSM Port: 05000
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	HSM Gateway(s): 0.0.0.0 ::
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	Software Versions:
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	BBL 010 ABL 011 App 023
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	CPLD Version:
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	1.9
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	SCR Firmware Version:
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	OROS-R2.99-R1.20
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	HmcListener: Created IPv4 socket 10 on port 3000.
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:04+0000	ttyS0	HmcListener: Created IPv6 socket 11 on port 3000.
2018-11-15T19:30:04+0000	ttyS0
2018-11-15T19:30:05+0000	ttyS0	Audit on 15/11/2018 18:22:08 00100003
2018-11-15T19:30:05+0000	ttyS0
2018-11-15T19:36:14+0000	ttyS0	Audit on 15/11/2018 18:28:18 00200069 0880004A83B3296D
2018-11-15T19:36:14+0000	ttyS0
2018-11-15T19:36:46+0000	ttyS0	Audit on 15/11/2018 18:28:47 00200069 0880004A7B33296D
2018-11-15T19:36:46+0000	ttyS0
2018-11-15T19:37:16+0000	ttyS0	Audit on 15/11/2018 18:29:20 00200069 0880004A7B73296D
2018-11-15T19:37:16+0000	ttyS0
2018-11-15T19:37:20+0000	ttyS0
2018-11-15T19:37:20+0000	ttyS0
2018-11-15T19:37:20+0000	ttyS0	TcpListener: Created IPv4 socket 15 on port 5000.
2018-11-15T19:37:20+0000	ttyS0
2018-11-15T19:37:20+0000	ttyS0
2018-11-15T19:37:20+0000	ttyS0
```

```
2018-11-15T19:37:20+0000 ttyS0  TcpListener: Created IPv6 socket 16 on port 5000.
2018-11-15T19:37:20+0000 ttyS0
2018-11-15T19:37:20+0000 ttyS0  Audit on 15/11/2018 18:29:24 00100002
2018-11-15T19:37:20+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0  CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:43:08+0000 ttyS0  TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-11-15T19:43:08+0000 ttyS0
2018-11-15T19:50:32+0000 ttyS0
2018-11-15T19:50:32+0000 ttyS0
2018-11-15T19:50:32+0000 ttyS0  CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-11-15T19:50:32+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0  CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:52:21+0000 ttyS0  TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-11-15T19:52:21+0000 ttyS0
2018-11-15T19:54:10+0000 ttyS0
2018-11-15T19:54:10+0000 ttyS0
2018-11-15T19:54:10+0000 ttyS0  CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-11-15T19:54:10+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0  CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:55:02+0000 ttyS0  TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-11-15T19:55:02+0000 ttyS0
2018-11-15T19:56:14+0000 ttyS0
2018-11-15T19:56:14+0000 ttyS0
2018-11-15T19:56:14+0000 ttyS0  CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-11-15T19:56:14+0000 ttyS0
2018-11-15T19:57:01+0000 ttyS0
2018-11-15T19:57:01+0000 ttyS0
2018-11-15T19:57:01+0000 ttyS0  TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2018-11-15T19:57:01+0000 ttyS0
2018-11-15T19:57:01+0000 ttyS0
```

```
2018-11-15T19:57:01+0000        ttyS0
2018-11-15T19:57:01+0000        ttyS0   CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2018-11-15T19:57:01+0000        ttyS0
2018-11-15T19:57:01+0000        ttyS0
2018-11-15T19:57:01+0000        ttyS0
2018-11-15T19:57:01+0000        ttyS0   TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2018-11-15T19:57:01+0000        ttyS0
2018-11-15T19:58:14+0000        ttyS0
2018-11-15T19:58:14+0000        ttyS0
2018-11-15T19:58:14+0000        ttyS0   CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2018-11-15T19:58:14+0000        ttyS0
2018-11-15T20:09:18+0000        ttyS0   Audit on 15/11/2018 19:01:21 00200069 0880004A7B33296D
2018-11-15T20:09:18+0000        ttyS0
2018-11-15T20:09:43+0000        ttyS0   Audit on 15/11/2018 19:01:47 00200069 0880004A7B73296D
2018-11-15T20:09:43+0000        ttyS0
2018-11-15T20:09:59+0000        ttyS0   Audit on 15/11/2018 19:02:03 0020006a
2018-11-15T20:09:59+0000        ttyS0
2018-11-15T20:10:36+0000        ttyS0   Audit on 15/11/2018 19:02:39 00200069 0880004A83B3296D
2018-11-15T20:10:36+0000        ttyS0
2018-11-15T20:10:41+0000        ttyS0
2018-11-15T20:10:41+0000        ttyS0
2018-11-15T20:10:41+0000        ttyS0   TcpListener: Closed IPv4 socket 15 on port 5000.
2018-11-15T20:10:41+0000        ttyS0
2018-11-15T20:10:41+0000        ttyS0
2018-11-15T20:10:41+0000        ttyS0
2018-11-15T20:10:41+0000        ttyS0   TcpListener: Closed IPv6 socket 16 on port 5000.
2018-11-15T20:10:41+0000        ttyS0
2018-11-15T20:10:42+0000        ttyS0   Audit on 15/11/2018 19:02:45 00100003
2018-11-15T20:10:42+0000        ttyS0
```

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: a) `cd /tmp` b) `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder.	SR	20:29
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.	SR	20:30
20	CA places 2 HSMFD, 2 OS DVD, 1 paper with printed HSMFD hash into a prepared TEB, then seals it.	SR	20:32
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 # BB46584689**	SR	20:33

Distribute the HSMFDs

Step	Activity	Initials	Time
22	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and for process review).	SR	20:33

Return the Laptop to TEB

Step	Activity	Initials	Time
23	CA places the laptop into a prepared TEB, then seals it.	SR	20:35
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 # BB81420094 / Service Tag # J8SVSG2**	SR	20:37

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. **CO4: Robert Seastrom** **OP TEB # BB46584684** **CO5: Christopher Griffiths** **OP TEB # BB46584685** **CO6: Gaurab Upadhaya** **OP TEB # BB46584686**	SR	20:41 20:45

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO4	OP 4 of 7	BB46584684	Robert Seastrom		2018 Nov 15	2041	SK
CO5	OP 5 of 7	BB46584685	Christopher Griffiths		2018 Nov 15	2043	SK
CO6	OP 6 of 7	BB46584686	Gaurab Upadhaya		2018 Nov 15	2044	SK

Return the Equipment to Safe #1

Step	Activity	Initials	Time
26	CA and IW brings a cart and escorts SSC1 into the safe room.	SR	20:46
27	SSC1 opens Safe #1 while shielding the combination from the camera.	SR	20:46
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.**	SR	20:47
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. **HSM4: TEB # BB51184680 / Serial # H1411011** **Laptop2: TEB # BB51184681 / Serial # 35063364997** **Laptop3: TEB # BB81420094 / Service Tag # J8SVSG2** **OS DVD (release 20170403): TEB # BB46584688** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584689**	SR	20:51

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.	SR	20:52
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.	SR	20:52
32	CA, SSC1 and IW leaves the safe room with the cart, closing the door behind them.	SR	20:53

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.	SR	20:54
34	SSC2 opens Safe #2 while shielding the combination from the camera.	SR	20:55
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.**	SR	20:55

CO Returns the Credentials to Safe #2

Step	Activity	Initials	Time
36	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. **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584684** **CO5: Christopher Griffiths** **Box # 1240** 20:58 **OP TEB # BB46584685** **CO6: Gaurab Upadhaya** 21:00 **Box # 1261** **OP TEB # BB46584686**	SR	21:00

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.	SR	21:00
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.	SR	21:01
39	CA, IW, SSC2, and COs leave safe room closing the door behind them.	SR	21:01

Act 6. Close the Key Signing Ceremony

The CA will finish the ceremony by:

- Reading any exceptions that may have occurred during the ceremony
- Calling the ceremony participants to sign the IW's script
- Stopping the online streaming and video recording
- Ensuring that all participants are signed out of the ceremony room log and escorted out of the ceremony room
- Preparing the audit bundle materials

Participants Signing of IW's Script

Step	Activity	Initials	Time
1	CA reads the exceptions that may have occurred during the ceremony.	SR	21:04
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.	SR	21:06
3	CA reviews IW's script, then signs the participants list.	SR	21:10

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.	SR	21:10

Post Ceremony Information

Step	Activity	Initials	Time
5	CA informs onsite participants about post ceremony activities.	SR	21:12

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.	SR	21:18
7	CA notifies the SA to stop the audit camera video recording.	SR	21:19

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: **20180411 00:00:00 to 20181116 00:00:00 UTC** e) IW's attestation (Appendix C). f) SA's attestation (Appendix D and E). All TEBs are labeled **Root DNSSEC KSK Ceremony 35**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	SR	22:56

Appendix A. References

The numeric items listed below has been referenced in the script.

[1] **coen-0.4.0:** The Ceremony Operating ENvironment (COEN) is a *Reproducible* ISO image consisting of a live operating system.
More information and the OS image source code can be found at https://github.com/iana-org/coen

[2] **`sha2wordlist:`** Is an application written in C by Kirei AB, which digests STDIN and output a SHA-256 checksum displayed as PGP words.
The source code is available at https://github.com/kirei/sha2wordlist

[3] **`hsmfd-hash:`** Is a bash script used to calculate, print and compare SHA-255 checksums for the HSMFD flash drives. It has the following options:

a) **`-c Calculate the HSMFD SHA-256 hash and PGP Word List`**

b) **`-p Print the calculated HSMFD SHA-256 hash and PGP Word List using the default printer`**

c) **`-m Compare the calculated SHA-256 hashes between HSMFDs`**

The following is the main command invoked by this script:
`find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist`
Note: The sort command has a different behavior depending on the locale settings specified in environment variables. Current OS coen-0.4.0 locale setting is `LC_COLLATE="POSIX"`

The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

[4] **`configure-printer:`** Is a bash script used to install the HP LaserJet printer from the command line instead using system-config-printer.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

[5] **`ping hsm:`** The HSM static IP address **`192.168.0.2`** it has been included in the **`/etc/hosts`** file.

[6] **`ksrsigner:`** Is an application written in C by Dr. Richard Lamb, which uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.
The source code is available at https://github.com/iana-org/dnssec-keytools

[7] **`printlog:`** Is a bash script use to print the *Key Signing Log* output from **`ksrsigner`** application.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

* A debian package is an **`ar`** archive. To extract data from a deb package, use the command **`ar -x ksk-tools-0.1.0coen_amd64.deb`**
Then extract the files with **`tar -zxvf data.tar.xz`**
The file will be located in the directory: **`./opt/icann/bin/`**

Appendix B. Audit Bundle Checklist

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

2. Key Ceremony Script (by IW)

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

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.

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.

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 D.

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 E. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

7. Other items

If applicable.

Appendix C. 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: **Shauna Royston**

Signature: 

Date: 2018 Nov 15

Appendix D. 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:

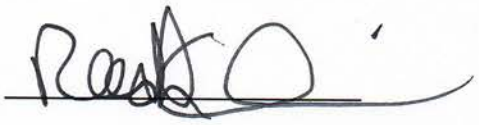
a) There were NO discrepancies found on the system configurations, assigned authorizations and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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: **20180411 00:00:00 to 20181116 00:00:00 UTC.**

SA: Reed Quinn

Signature: 

Date: 2018 Nov 15

Appendix E. 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: Reed Quinn

Signature: 

Date: 2018 Nov 15

```
## Last commit: 2018-11-02 23:45:58 UTC by bmartin
version 12.3X48-D65.1;
system {
    host-name srx;
    domain-name ksk.cjr.dns.icann.org;
    location {
        country-code US;
        postal-code 22701;
        building Terramark-Admin;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## 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 "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrik Tudor";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## 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-cjr;
            }
        }
        gateway Gateway-to-KMF-West {
            ike-policy ike-policy-KMF;
            address 192.0.35.202;
            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-West {
            bind-interface st0.1;
            ike {
                gateway Gateway-to-KMF-West;
                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_east_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_west_acs kmf_west_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 ipsec to-zone access {
    policy allow-ipsec-to-access {
        match {
            source-address [ kmf_west_acs kmf_west_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_west_access;
            destination-address kmf_east_access;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone video to-zone ipsec {
    policy allow-video-to-ipsec {
        match {
            source-address VSS;
            destination-address kmf_west_vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-access-video {
```

```
            match {
                source-address kmf_east_video;
                destination-address kmf_west_video;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone guest to-zone untrust {
        policy allow-guest-to-untrust {
            match {
                source-address kmf_east_guest;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone wifi to-zone untrust {
        policy allow-wifi-to-untrust {
            match {
                source-address kmf_east_wifi;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone ipsec to-zone video {
        policy allow-ipsec-to-video {
            match {
                source-address kmf_west_vss;
                destination-address 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 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 10.4.29.203/32;
            address ACC 10.4.29.202/32;
            address IDP 10.4.29.201/32;
            address EVM 10.4.29.200/32;
            address IMS 10.4.29.204/32;
            address E1 10.4.29.210/32;
            address E2 10.4.29.211/32;
            address E3 10.4.29.212/32;
            address E4 10.4.29.213/32;
            address kmf_east_access 10.4.29.192/26;
```

```
        address localnet 10.4.29.0/24;
        address-set iris-scanners {
            address E1;
            address E2;
            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_east_video 10.4.29.128/26;
        address VSS 10.4.29.150/32;
        address C1 10.4.29.151/32;
        address C2 10.4.29.152/32;
        address C3 10.4.29.153/32;
        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 10.4.29.20/32;
        address VCC 10.4.29.22/32;
        address kmf_east_guest 10.4.29.0/25;
    }
    interfaces {
        vlan.2 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
```

```
                }
            }
        }
        security-zone ipsec {
            address-book {
                address kmf_west_access 10.4.28.192/26;
                address kmf_west_video 10.4.28.128/26;
                address kmf_west_acs 10.4.28.204/32;
                address kmf_west_acc 10.4.28.202/32;
                address kmf_west_idp 10.4.28.201/32;
                address kmf_west_evm 10.4.28.200/32;
                address kmf_west_ims 10.4.28.203/32;
                address kmf_west_E1 10.4.28.210/32;
                address kmf_west_E3 10.4.28.212/32;
                address kmf_west_E4 10.4.28.213/32;
                address kmf_west_vss 10.4.28.150/32;
                address kmf_west_C1 10.4.28.151/32;
                address kmf_west_C2 10.4.28.152/32;
                address kmf_west_C3 10.4.28.153/32;
            }
            interfaces {
                st0.1 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                            ike;
                            ssh;
                        }
                    }
                }
            }
        }
        security-zone wifi {
            address-book {
                address kmf_east_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";
    }
    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 152.194.1.148/28;
            }
        }
    }
    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 10.4.29.193/26;
            }
        }
        unit 1 {
            family inet {
                address 10.4.29.129/26;
            }
        }
        unit 2 {
            family inet {
                address 10.4.29.1/25;
            }
        }
    }
}
```

```
routing-options {
    static {
        route 0.0.0.0/0 next-hop 152.194.1.145;
        route 10.4.28.0/24 next-hop st0.1;
        route 192.0.35.202/32 next-hop 152.194.1.145;
    }
}
policy-options {
    prefix-list resolver-servers {
        8.8.4.4/32;
        8.8.8.8/32;
    }
    prefix-list local-prefixes {
        10.4.29.0/24;
    }
    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 {
                        192.0.35.202/32;
                        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;
    }
}
```