Root DNSSEC KSK Ceremony 33

Wednesday April 11, 2018

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

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

Abbreviations

AUD = Third Party Auditor
CA = Ceremony Administrator
CO = Crypto Officer
EW = External Witness
FD = Flash Drive
HSM = Hardware Security Module
IW = Internal Witness
KMF = Key Management Facility
KSR = Key Signing Request
OP = Operator
PTI = Public Technical Identifiers
RKSH = Recovery Key Share Holder
RKOS = RZ KSK Operations Security
RZM = Root Zone Maintainer
SA = System Administrator
SKR = Signed Key Response
SMK = Storage Master Key
SO = Security Officer
SSC = Safe Security Controller
SW = Staff Witness
TCR = Trusted Community Representative
TEB = Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20)

Participants

Key Ceremony roles are described on https://www.iana.org/help/key-ceremony-roles
Instructions: At the end of the ceremony, participants sign on IW's copy. IW records time upon completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Matthew Larson / ICANN		2018 Apr 11	20:10
IW	Jonathan Denison / ICANN			
SSC1	James Cole / ICANN			
SSC2	Carlos Reyes / ICANN			
CO3	Olaf Kolkman			
CO4	Robert Seastrom			
CO5	Christopher Griffiths			
CO6	Gaurab Upadhaya			
CO7	Alain Aina			
RZM	Duane Wessels / Verisign			
RZM	Ryan Brown / Verisign			
RZM	Alexander Brown / Verisign			
AUD	Chris Koucheki / RSM			
AUD	Matthew Kleckner / RSM			
SA	Reed Quinn / ICANN			
SA	Brian Martin / ICANN			
RKOS / CA Backup	Alberto Duero / PTI			
RKOS / IW Backup	Andres Pavez / PTI			
SW	Marilia Hirano / PTI			
SW	Shaunte Anderson / PTI			
EW	Smiljana Antonijevic			

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

Note: The CA leads the ceremony. Only CAs, IWs, or SAs can enter and escort other participants into the Ceremony room. Dual Occupancy is enforced. IW with CA or SA must remain inside the Ceremony room if participants are present in that room. CAs, IWs or SAs may escort participants out of the Ceremony room at the CA's discretion only if the Safe room is not occupied during ceremony. All participants are required to sign in and out of the Ceremony room using the visitor log. The SA starts filming before the participants enter the Ceremony room.

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

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

Act 1. Initiate Ceremony and Retrieve Equipment

Sign into the Key Ceremony Room

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.	JD	17:00
2	CA confirms that all participants are signed into the Ceremony Room, then performs a roll call using the participants list on page 2.	JD	17:02

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3	CA reviews the emergency evacuation procedure with onsite participants.	JD	17:02
4	CA explains the use of personal electronic devices during ceremony.	JD	17:03
5	CA briefly explains the purpose of the ceremony.	JD	17:05

Verify the Time and Date

Step	Activity	Initials	Time
6	IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2018/4/11 17:05 All entries into this script or any logs should follow this common source of time.	JD	17:05

Open the Credential Safe #2

Step	Activity	Initials	Time
7	CA and IW brings a flashlight and escorts the SSC2 and the COs into the safe room.	JD	17:06
8	SSC2 opens Safe #2 while shielding the combination from the camera.	JD	17:08
9	Complete the safe log by following the steps below: 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.	JD	17:10

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 1 Step(s): 60 Page(s): 5 Date and Time: 2018/4/11 17:26	JD	17:36
2.	IW describes the exception(s) and action(s) below.	JD	17:36

FOR C05/C07: ERROR IN CURRENT SCRIPT - REFERENCES #'S FROM CEREMONY 31 THAT WERE UNUSED. CONTINUITY OF #'S CAN BE SEEN BY REFERENCING THE CEREMONY 29. NEW NUMBERS RECORDED IN CEREMONY 33 SCRIPT. OF THE NUMBERS HAVE BEEN CORRECTED

COs Extract the Credentials From the Safe Deposit Boxes

Step	Activity	Initials	Time
10	One by one, the selected CO retrieves the required TEBs by following the steps below: 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. **CO3: Olaf Kolkman** **Box # 1239** **OP TEB # BB46584464 (Retain)** ✓ **SO TEB # BB46584594 (Check and Return)** ✓ **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB46592028 (Retain)** ✓ **SO TEB # BB46584596 (Check and Return)** ✓ **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46592027 (Retain)** ? Exception BB46584466 **SO TEB # BB46584598 (Check and Return)** ✓ **CO6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB46584467 (Retain)** ✓ **SO TEB # BB21907207 (Check and Return)** ✓ **CO7: Alain Aina** **Box # 1242** **OP TEB # BB46592125 (Retain)**? BB46584468 Exception **SO TEB # BB46584600 (Check and Return)** ✓	JO	17:26

Close the Credential Safe #2

Step	Activity	Initials	Time
11	Once all deposit boxes are closed and locked, SSC2 writes the date, time and signature on the safe log where "Close Safe" is indicated. IW verifies the entry then initials it.	JD	17:27
12	SSC2 returns the safe log back in the Safe #2 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW verifies that the safe is locked and the "WAIT" light indicator is off.	JD	17:27
13	CA, IW, SSC2, and COs leave the safe room with TEBs, closing the door behind them.	JD	17:28

Open Equipment Safe #1

Step	Activity	Initials	Time
14	CA and IW brings a cart and escorts the SSC1 into the safe room.	JD	17:37
15	SSC1 opens Safe #1 while shielding the combination from the camera.	JD	17:38
16	Complete the safe log by following the steps below: 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.	JD	17:39

Remove the Equipment from Safe #1

Step	Activity	Initials	Time
17	CA extracts each equipment from the safe by following the steps below: a) CAREFULLY remove the equipment TEB from the safe. b) Read out the TEB number, then verify its integrity while showing it to the audit camera. c) Place the 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 # BB51184621 / Serial # H1403032 (Place on cart)** ✓ **HSM4: TEB # BB51184628 / Serial # H1411011 (Check and Return)** ✓ **Laptop1: TEB # BB51184616 / Serial # 41593712005 (Place on cart)** ✓ **Laptop2: TEB # BB51184630 / Serial # 35063364997 (Check and Return)** ✓ **OS DVD (release 20170403) + HSMFD: TEB # BB46592032 (Place on cart)** ✓	JD	17:44

Close the Equipment Safe #1 and exit the Safe Room

Step	Activity	Initials	Time
18	SSC1 writes the date, time and signature on the safe log where Close Safe is indicated. IW verifies the safe log entry then initials it.	JD	17:45
19	SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW verifies that the safe is locked and the "WAIT" light indicator is off.	JD	17:45
20	CA, IW and SSC1 leaves the safe room with the cart, closing the door behind them.	JD	17:46

Act 2. Setup Equipment

Setup Laptop

Step	Activity	Initials	Time
1	CA prepares each equipment by following the steps below: a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read out the TEB number and the serial number (if applicable) while IW matches it with the prior ceremony script in this facility. d) Remove and discard the TEB, then place the equipment on its designated area on the ceremony table. **HSM3: TEB # BB51184621 / Serial # H1403032** **Laptop1: TEB # BB51184616 / Serial # 41593712005** **OS DVD (release 20170403) + HSMFD: TEB # BB46592032**	JD	17:50
2	CA boots the laptop by following the steps below: a) Connect the USB printer cable and USB null modem cable into the bottom USB slots on each side of the laptop. b) Connect the external display, then the power supply c) Immediately insert the **OS DVD release 20170403** after the laptop power is switched ON.	JD	17:53
3	CA sets up the laptop by following the steps below: a) Press `Ctrl+Alt+F2` to get a console prompt and log in as `root` b) Execute `system-config-display --noui` c) Execute `killall Xorg` d) Confirm that the external display works. e) Log in as `root`	JD	17:56

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 2 Step(s): 5 Page(s): 9 Date and Time: 2018/4/11 17:59	JD	17:59
2.	IW describes the exception(s) and action(s) below.	JD	18:01

KNOCK OF OUTSIDE DOOR BY FACILITY ADMINISTRATORS. HAD TO PAUSE CEREMONY TO ADDRESS CONCERNS.

Setup Printer

Step	Activity	Initials	Time
4	CA confirms that the printer is switched ON, then configures it through: **System > Administration > Printing** CA then performs the following steps to configure the printer and to print a test page: a) Click the **New Printer** icon (left side), leave everything default, then click the button **Forward.** b) Under "Select Connection" choose the *first device* **HP Laserjet xxxx** then click the button **Forward.** **Note: The xxxx is the printer model.** c) Select **HP** and click the button **Forward.** d) Under "Models" scroll up and select **Laserjet**, then click the button **Forward.** e) Click the button **Apply** to finish. f) Under "Local Printers" from the left menu, select **printer**. g) Click the button **Make Default Printer** and **Print Test Page**. h) Close the printer setup window.	JD	17:59

Setup Date

Step	Activity	Initials	Time
5	CA opens a terminal window through: **Applications > Accessories > Terminal** CA then performs the following steps to increase its visibility: a) Click the **View** menu and select **Zoom In.** b) Repeat the step above as necessary.	JD	18:02
6	CA updates the date and time on the laptop while referencing from the clock. Using the terminal window, CA executes the following: `date -s "20180411 HH:MM:00"` where `HH` is two-digit Hour, `MM` is two-digit Minutes and `00` is Zero Seconds. CA executes `date` using the terminal window to confirm the date is properly configured.	JD	18:02

Format and label the blank FD

Step	Activity	Initials	Time

7	CA formats a new FD by following the steps below:
	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 perform the following steps:
	c) Confirm the drive letter by executing:
	`df`
	d) Unmount the drive by executing:
	`umount /dev/sda1`
	e) Format and label the FD by executing:
	`mkfs.vfat -n HSMFD -I /dev/sda1`
		JD	18:04

8	CA repeats step 7 for the 2nd blank FD.	JD	18:04
9	CA repeats step 7 for the 3rd blank FD.	JD	18:05
10	CA repeats step 7 for the 4th blank FD.	JD	18:06
11	CA repeats step 7 for the 5th blank FD.	JD	18:06

Connect the HSMFD

Step	Activity	Initials	Time
12	CA plugs the **Ceremony 31 HSMFD** into the USB slot, then performs the following steps: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window. d) Place the unused **HSMFD 31** on the FD holder.	JD	18:08
13	CA calculates the SHA-256 hash of the HSMFD contents by executing: `hsmfd-hash -c` IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 31 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: 5458388f495d9682448482fd69f3b1f4f06ae7eafe04a034dddf8fcc43ed6f71 PGP Words: eating everyday classic midsummer deckhand filament prefer Istanbul crumpled Jupiter miser Wyoming gazelle vertigo sailboat Virginia unearth hamburger transit unaunted woodlark alkali ragtime confidence swelter therapist payday revolver crucial unify gremlin hideaway	JD	18:09

Start the Terminal Session Logging

Step	Activity	Initials	Time
14	CA changes the default directory to HSMFD by executing: `cd /media/HSMFD`	JD	18:10
15	CA starts capturing the terminal session by executing: `script script-20180411.log`	JD	18:10

Start the HSM Activity Logging

Step	Activity	Initials	Time
16	CA opens a second terminal window through: **Applications > Accessories > Terminal.** CA then performs the following steps to increase its visibility: a) Click the **View** menu and select **Zoom In.** b) Repeat the step above as necessary.	JD	18:10

17	CA performs the following to capture the activity logs of the HSM through the serial port:
	a) Switch directory to HSMFD by executing:
	`cd /media/HSMFD`
	b) Set the serial port baud rate by executing:
	`stty -F /dev/ttyUSB0 115200`
	c) Start logging the serial output by executing:
	`ttyaudit /dev/ttyUSB0`
	Note: DO NOT unplug the USB null modem cable from the laptop as this will stop capturing activity logs from the serial port.
		JD	18:11

Power Up the HSM

Step	Activity	Initials	Time
18	CA prepares the HSM by following the steps below: a) Plug the USB null modem serial cable to the HSM. b) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** c) Scroll the logging screen up and look for the HSM serial number. d) IW matches the displayed HSM serial number on the screen with the information below. **HSM3: Serial # H1403032** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	JD	18:12

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 3 Step(s): 1 Page(s): 12 Date and Time: 2018/4/11 18:19	JD	18:24
2.	IW describes the exception(s) and action(s) below.	JD	18:24

THE BAG HE'S WERE NOT READ ALOUD FOR:

C03
C04
C05

AFTER NOTING THIS, BAGS WERE READ ALOUD.

SUBSEQUENTLY, ~~C06~~ C06, C07 WERE READ ALOUD.

FUTURE SCRIPTS SHOULD NOTE THE NEED FOR READING ALOUD.

ADDITION OF THIS STEP WILL VERIFY CONTINUITY/CHAIN BETWEEN TIERS 3 TO 4.

Act 3. Activate HSM and Generate Signatures

Enable/Activate the HSM

Step	Activity	Initials	Time
1	One by one, CA calls each COs listed below to perform the following steps: a) CA and CO inspects the TEB 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. **CO3: Olaf Kolkman** ✓ **OP TEB # BB46584464** **CO4: Robert Seastrom** ✓ **OP TEB # BB46592028** **CO5: Christopher Griffiths** × **OP TEB # ~~BB46592027~~** EXCEPTION **CO6: Gaurab Upadhaya** ✓ **OP TEB # BB46584467** **CO7: Alain Aina** × **OP TEB # ~~BB4659212~~5** EXCEPTION	JD	18:25
2	CA activates the **HSM** by following the steps below: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, hit **ENT** to confirm. c) 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 3 of 7 2nd OP card 4 of 7 3rd OP card 5 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	JD	18:30

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.	JO	18:30

4	CA performs the following steps to test the network connectivity between laptop and HSM:
	a) Switch to the terminal window
	b) Test connectivity by executing:
	`ping 192.168.0.2`
	c) Wait for responses, then exit by pressing:
	`Ctrl + C`
		JO	18:31

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 is for the normal operation and 3 are for fallback scenarios.**	JO	18:32

Execute the KSR Signer for Phase D to E

Step	Activity	Initials	Time
6	CA executes the following command to sign the KSR file: `ksrsigner /media/KSR/KSK33-0-D_to_E/ksr-root-2018-q3-0-d_to_e.xml`	JO	18:32
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.	JO	18:33

Verify the KSR Hash for Phase D to E

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed on the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify himself/herself in front of the room and provide documents for IW to review. b) RZM representative reads out the PGP word list SHA-256 hash of the KSR file being used. c) IW retains the documents provided by the RZM representative and writes the name below: ALEXANDER BROWN	JD	18:35
9	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	JD	18:35
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/KSK33-0-D_to_E/skr-root-2018-q3-0-d_to_e.xml`	JD	18:36

Execute the KSR Signer for Phase E to D

Step	Activity	Initials	Time
11	CA executes the following command to sign the KSR file: `ksrsigner /media/KSR/KSK33-1-E_to_D/ksr-root-2018-q3-1-e_to_d.xml`	JD	18:36
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.	JD	18:37

Verify the KSR Hash for Phase E to D

Step	Activity	Initials	Time
13	When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	JD	18:37
14	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	JD	18:38
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/KSK33-1-E_to_D/skr-root-2018-q3-1-e_to_d.xml`	JD	18:38

VERISIGN

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

VerisignInc.com

April 11th, 2018

To Whom It May Concern:

This is a letter of Verification of Employment for Alexander Brown. Verisign, Inc. has employed Alexander Brown full-time since September 19th, 2016, currently as an Engineer II - CBO in our Production Operations organization.

Verisign is the trusted provider of Internet infrastructure services and operates the authoritative directory of all .com, .net, .cc, .tv, and .name domain names and the back-end systems for all .gov, .jobs and .edu domain names.
Verisign manages and protects the global domain name system (DNS) infrastructure for more than 113 million domain names and processes approximately 60 billion queries daily, while maintaining 100 percent operational accuracy and stability for more than a decade. Our services also help ensure that online businesses are as available as the Web itself.

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

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

Sincerely,

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

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

verisign.com

11 April 2018

The SHA256 hash of the 2018 Q3 KSR file is:

ksr-root-2018-q3-0-d_to_e.xml:

**9515e2b07dd11ce670183630081e6562b0e4705e56e9d8fe2fc5
5cca3cc33c5f**

The PGP wordlist for the hash above is:

**preclude bifocals tiger phonetic klaxon scavenger
befriend trombonist guidance borderline Christmas
commando aimless Burlington fracture gadgetry ruffled
tradition guidance finicky egghead ultimate stormy
yesteryear cement resistor escape revenue cobra replica
cobra forever**

Attested on behalf of VeriSign by:

Alexander Brown
Cryptographic Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK33-0-D_to_E/ksr-root-2018-q3-0-d_to_e.xml (at Wed Apr 11 18:32:03 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-0-D_to_E/ksr-root-2018-q3-0-d_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
9515E2B07DD11CE670183630081E6562B0E4705E56E9D8FE2FC55CCA3CC33C5F
>> preclude bifocals tiger phonetic klaxon scavenger befriend trombonist guidance borderline Christmas commando aiml
ess Burlington fracture gadgetry ruffled tradition guidance finicky egghead ultimate stormy yesteryear cement resist
or escape revenue cobra replica cobra forever <<

Reading KSK schedule "rollover(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/P,20326(Klajeyz)/S
3 19036(Kjqmt7v)/P,20326(Klajeyz)/S
4 19036(Kjqmt7v)/P,20326(Klajeyz)/S
5 19036(Kjqmt7v)/P,20326(Klajeyz)/S
6 19036(Kjqmt7v)/P,20326(Klajeyz)/S
7 19036(Kjqmt7v)/P,20326(Klajeyz)/S
8 19036(Kjqmt7v)/P,20326(Klajeyz)/S
9 19036(Kjqmt7v)/P,20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK33-0-D_to_E/skr-root-2018-q3-0-d_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt7v)/P

SHA256 hash of SKR:
59ADDD6C6D8EB19545DB9871F256049168215550181269B549DD961CF73434F7
>> endow perceptive swelter handiwork goggles microwave sailboat Montana crusade suspicious printer hideaway uproot
escapade adrift miracle frighten Camelot edict embezzle beaming backwater gazelle positive deckhand tambourine prefe
r Brazilian virus confidence choking voyager <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

VERISIGN

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

verisign.com

11 April 2018

The SHA256 hash of the 2018 Q3 KSR file is:

ksr-root-2018-q3-1-e_to_d.xml:

9949389f5c69e76dc0cec8a92b75a8bb7e5423fbf03a8be800ecf59f2ce44367

The PGP wordlist for the hash above is:

prowler dinosaur classic opulent escape guitarist transit hazardous slowdown sardonic spaniel passenger briefcase impartial retouch publisher locale equation blowtorch Wichita unearth corrosion obtuse typewriter aardvark unicorn vapor opulent Burbank tradition crucial graduate

Attested on behalf of VeriSign by:

Alexander Brown
Cryptographic Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK33-1-E_to_D/ksr-root-2018-q3-1-e_to_d.xml (at Wed Apr 11 18:36:07 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-1-E_to_D/ksr-root-2018-q3-1-e_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
9949389F5C69E76DC0CEC8A92B75A8BB7E5423FBF03A8BE800ECF59F2CE44367
>> prowler dinosaur classic opulent escape guitarist transit hazardous slowdown sardonic spaniel passenger briefcase
 impartial retouch publisher locale equation blowtorch Wichita unearth corrosion obtuse typewriter aardvark unicorn
vapor opulent Burbank tradition crucial graduate <<

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/KSK33-1-E_to_D/skr-root-2018-q3-1-e_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
13DEF14FDF19C450A791AE6319A4F1C4A5DED3E978C43F55CA754CE543B57AD7
>> Aztec telephone unwind document talon bottomless snowslide embezzle repay miracle robust Galveston bedlamp Pandor
a unwind reproduce reindeer telephone stapler ultimate island reproduce cowbell equipment spellbind impartial draina
ge travesty crucial positive keyboard stethoscope <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Execute the KSR Signer for Phase D to D

Step	Activity	Initials	Time
16	CA executes the following command to sign the KSR file: `ksrsigner /media/KSR/KSK33-2-D_to_D/ksr-root-2018-q3-2-d_to_d.xml`	JD	18:38
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.	JD	18:39

Verify the KSR Hash for Phase D to D

Step	Activity	Initials	Time
18	When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	JD	18:39
19	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	JD	18:39
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/KSK33-2-D_to_D/skr-root-2018-q3-2-d_to_d.xml`	JD	18:40

Execute the KSR Signer for Phase C to C

Step	Activity	Initials	Time
21	CA executes the following command to sign the KSR file: `ksrsigner /media/KSR/KSK33-3-C_to_C/ksr-root-2018-q3-3-c_to_c.xml`	JD	18:40
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.	JD	18:40

Verify the KSR Hash for Phase C to C

Step	Activity	Initials	Time
23	When the program requests verification of the KSR hash, the CA asks the RZM representative to read out the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	JD	18:41
24	Participants confirm that the hash displayed on the terminal window matches with the RZM read out, then CA asks **"are there any objections?"**	JD	18:42
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/KSK33-3-C_to_C/skr-root-2018-q3-3-c_to_c.xml`	JD	18:42

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

verisign.com

11 April 2018

The SHA256 hash of the 2018 Q3 KSR file is:

ksr-root-2018-q3-2-d_to_d.xml:

12e17cecd65ae156955c71bf3b002983dc1d47ec533aab73bad0769ef96656eb

The PGP wordlist for the hash above is:

atlas tolerance kiwi unicorn stockman existence tempest escapade preclude fascinate hamlet rebellion clockwork adroitness breakup Jamaica sweatband breakaway dashboard unicorn dwelling corrosion rhythm hurricane shadow savagery inverse onlooker waffle gossamer egghead underfoot

Attested on behalf of VeriSign by:

Alexander Brown
Cryptographic Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK33-2-D_to_D/ksr-root-2018-q3-2-d_to_d.xml (at Wed Apr 11 18:38:14 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-2-D_to_D/ksr-root-2018-q3-2-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
12E17CECD65AE156955C71BF3B002983DC1D47EC533AAB73BAD0769EF96656EB
>> atlas tolerance kiwi unicorn stockman existence tempest escapade preclude fascinate hamlet rebellion clockwork ad
roitness breakup Jamaica sweatband breakaway dashboard unicorn dwelling corrosion rhythm hurricane shadow savagery i
nverse onlooker waffle gossamer egghead underfoot <<

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/KSK33-2-D_to_D/skr-root-2018-q3-2-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt7v)/S
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt7v)/S

SHA256 hash of SKR:
A05918310598659DA6B48265386CDA27B904D9676F1D749E48E3AD41A10E24E1
>> ragtime examine beaming company adult narrative fracture Ohio rematch politeness miser glossary classic handiwork
 surmount celebrate sentence alkali sugar graduate gremlin breakaway indoors onlooker deadbolt torpedo ringbolt deca
dence ratchet Atlantic bluebird tolerance <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

VERISIGN

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

verisign.com

11 April 2018

The SHA256 hash of the 2018 Q3 KSR file is:

ksr-root-2018-q3-3-c_to_c.xml:

65318a02b85022aee8596355858fa560add41c9ceaafdee1f0a81efa86b2c553

The PGP wordlist for the hash above is:

fracture company Oakland aftermath select embezzle blockade performance trauma examine flatfoot equipment music midsummer reindeer fortitude ringbolt souvenir befriend October Trojan pharmacy tactics tolerance unearth paramount berserk whimsical necklace pioneer solo enterprise

Attested on behalf of VeriSign by:

Alexander Brown
Cryptographic Engineer
Cryptographic Business Operations
VeriSign, Inc.

```
Starting: ksrsigner /media/KSR/KSK33-3-C_to_C/ksr-root-2018-q3-3-c_to_c.xml (at Wed Apr 11 18:40:01 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-3-C_to_C/ksr-root-2018-q3-3-c_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
65318A02B85022AEE8596355858FA560ADD41C9CEAAFDEE1F0A81EFA86B2C553
>> fracture company Oakland aftermath select embezzle blockade performance trauma examine flatfoot equipment music m
idsummer reindeer fortitude ringbolt souvenir befriend October Trojan pharmacy tactics tolerance unearth paramount b
erserk whimsical necklace pioneer solo enterprise <<

Reading KSK schedule "normal(2010)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
2 19036(Kjqmt7v)/S
3 19036(Kjqmt7v)/S
4 19036(Kjqmt7v)/S
5 19036(Kjqmt7v)/S
6 19036(Kjqmt7v)/S
7 19036(Kjqmt7v)/S
8 19036(Kjqmt7v)/S
9 19036(Kjqmt7v)/S
Generated new SKR in /media/KSR/KSK33-3-C_to_C/skr-root-2018-q3-3-c_to_c.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         19036(Kjqmt7v)/S
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         19036(Kjqmt7v)/S
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         19036(Kjqmt7v)/S
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         19036(Kjqmt7v)/S
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         19036(Kjqmt7v)/S
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         19036(Kjqmt7v)/S
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         19036(Kjqmt7v)/S
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   19036(Kjqmt7v)/S

SHA256 hash of SKR:
BEB2EFF282CFCC589D103D35FB2706BA7C8B04EA2A58BC05B319292DC486A5F1
>> skydive pioneer uncut vagabond miser Saturday spigot everyday quadrant autopsy commence conformist watchword cele
brate afflict puberty kiwi Medusa adrift undaunted brickyard everyday showgirl almighty scallion bottomless breakup
clergyman snowslide letterhead reindeer vacancy <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 3 Step(s): 30/31 Page(s): 66 Date and Time: 2018 / 4 / 11 18:59	JD	18:59
2.	IW describes the exception(s) and action(s) below.	JD	18:59

1. TTY AUDIT PROGRAM STOPPED AT 18:25
2. NOTICED AT 18:51
3. RESTARTED TTY AUDIT AT 18:59
4. TWO DIFFERENT TTY FILES DUE TO SCRIPT RESTARTS
5. NOTE: RECONSIDER CABLE ATTACHMENTS TO LAPTOP TO PREVENT DOSTLING OF USB

Print Copies of the Operation for Participants

Step	Activity	Initials	Time
26	CA prints out the KSR Signer log by executing the following command on the terminal window: `for i in $(ls -1 ksrsigner-20180411*.log); do printlog $i X; done` **Note: Replace "X" with the amount of copies needed for the participants.**	JD	18:44
27	IW attaches a copy of each ksrsigner log to his/her script.	JD	18:49

Backup the Newly Created SKR

Step	Activity	Initials	Time
28	CA copies the contents of the KSR FD by executing the following command on the terminal window: `cp -pR /media/KSR/* .` Confirm overwrite by entering "y" if prompted.	JD	18:49

29	CA uses the terminal window to execute the following commands:
	a) list the contents of the KSR FD by executing:
	`ls -ltrR /media/KSR`
	b) flush the system buffers by executing:
	`sync`
	c) unmount the KSR FD by executing:
	`umount /media/KSR`
		JD	18:50

30	CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative.	JD	18:50

Disable/Deactivate the HSM

Step	Activity	Initials	Time
31	CA ensures to utilize the unused OP cards to deactivate the **HSM**: a) CA displays the HSM activity logging terminal window b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"2.Set Offline"**, hit **ENT** to confirm. d) When **"Set Offline?"** is displayed, hit **ENT** to confirm. e) When **"Insert Card OP #?"** is displayed, insert the OP card from the card holder. f) When **"PIN?"** is displayed, enter **"11223344"**, then hit **ENT**. g) When **"Remove Card?"** is displayed, remove the OP card. h) Repeat steps e) to g) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **OFF.** IW records the used cards below. Each card is returned to card holder after use. 1st OP card 6 of 7 2nd OP card 7 of 7 3rd OP card 5 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	JD	19:03

Act 4. Secure Hardware

Return the HSM to TEB

Step	Activity	Initials	Time
1	CA switches the HSM to power OFF, then disconnects the power, serial and Ethernet connections from it. **Note: DO NOT unplug the cable connections on the laptop.**	JD	19:06
2	CA places the HSM into a prepared TEB, then seals it.	JD	19:07
3	CA performs the following steps: a) Read out the TEB number and HSM serial number, then shows it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB with IW using a ballpoint pen. d) Give IW the sealing strips for later inventory. e) Place the HSM TEB on the cart. **HSM3: TEB # BB51184645 / Serial # H1403032**	JD	19:08

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 USB null modem cable from the laptop. b) Stop logging the serial output **(ttyaudit)** by executing: `exit` c) Stop logging the terminal session by executing: `exit` **Note: The terminal session window will remain open.**	JD	19:09

Backup the HSMFD Contents

Step	Activity	Initials	Time
5	CA sets `dotglob` by executing the command below on the terminal window: `shopt -s dotglob` **Note: This enables copying of all files from the original HSMFD.**	JD	19:09
6	CA prints **2** copies of the hash by executing the following command on the terminal window **twice:** `hsmfd-hash -p` **Note: One copy for audit bundle and one copy for HSMFD package.**	JD	19:10
7	CA displays the contents of HSMFD by executing the following command on the terminal window: `ls -ltrR`	JD	19:10
8	CA plugs a blank FD labeled HSMFD into a free USB slot on the laptop, then waits for the OS to recognize it as **HSMFD_**	JD	19:11
9	CA closes the file system window, then creates a backup of the HSMFD by executing following command on the terminal window: `cp -pR * /media/HSMFD_`	JD	19:11
10	CA matches the SHA-256 hash between the original HSMFD and the copy HSMFD by executing the following command on the terminal window: `hsmfd-hash -m`	JD	19:12
11	CA unmounts the HSMFD copy by executing the following command on the terminal window: `umount /media/HSMFD_`	JD	19:12
12	CA removes the **HSMFD_** and places it on the holder.	JD	19:12
13	CA repeats step 8 to 12 for the 2nd copy.	JD	19:13
14	CA repeats step 8 to 12 for the 3rd copy.	JD	19:14
15	CA repeats step 8 to 12 for the 4th copy.	JD	19:15
16	CA repeats step 8 to 12 for the 5th copy.	JD	19:16

Print Logging Information

Step	Activity	Initials	Time

17	CA prints out a copy of the logging information by executing the following command on the terminal window:
	`enscript -2Gr -# 1 script-201804*.log`
	`enscript -Gr -# 1 --font="Courier8" ttyaudit-ttyUSB*-201804*.log`
	Attach the printed copies to IW script.
	Note: Ignore the error regarding non-printable characters if prompted.
		JD	19:17

HSMFD SHA-256 HASH **2018/04/11**

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

 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
```

```
Script started on Wed 11 Apr 2018 06:09:44 PM UTC
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=1.84 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.381 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.520 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=0.374 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=255 time=0.358 ms

--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.358/0.695/1.842/0.576 ms
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsi\007gner /media/KSR
/KSK33-0-D_to_E/ks\007r-root-2018-q3-0-d_
Starting: ksrsigner /media/KSR/KSK33-0-D_to_E/ksr-root-2018-q3-0-d_to_e.xml (at Wed Ap
r 11 18:32:03 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-0-D_to_E/ksr-root-2018-q3-0-d_to_e.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
9515E2B07DD11CE670183630081E6562B0E4705E56E9D8FE2FC55CCA3CC33C5F
>> preclude bifocals tiger phonetic klaxon scavenger befriend trombonist guidance bord
erline Christmas commando aimless Burlington fracture gadgetry ruffled tradition guida
nce finicky egghead ultimate stormy yesteryear cement resistor escape revenue cobra re
plica cobra forever <<
Is this correct (y/N)? y

Reading KSK schedule "rollover(2010,2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S,20326(Klajeyz)/P
2 19036(Kjqmt7v)/P,20326(Klajeyz)/S
3 19036(Kjqmt7v)/P,20326(Klajeyz)/S
4 19036(Kjqmt7v)/P,20326(Klajeyz)/S
5 19036(Kjqmt7v)/P,20326(Klajeyz)/S
6 19036(Kjqmt7v)/P,20326(Klajeyz)/S
7 19036(Kjqmt7v)/P,20326(Klajeyz)/S
8 19036(Kjqmt7v)/P,20326(Klajeyz)/S
9 19036(Kjqmt7v)/P,20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK33-0-D_to_E/skr-root-2018-q3-0-d_to_e.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/S,19036(Kjqmt
7v)/P

SHA256 hash of SKR:
59ADDD6C6D8EB19545DB9871F2560491682155501812 69B549DD961CF73434F7
>> endow perceptive swelter handiwork goggles microwave sailboat Montana crusade suspi
cious printer hideaway uproot escapade adrift miracle frighten Camelot edict embezzle
beaming backwater gazelle positive deckhand tambourine prefer Brazilian virus confiden
ce choking voyager <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180411-183203.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrsi\007gner /media/KSR
/KSK33-1-E_to_D/ks\007r-root-2018-q3-1-e_
Starting: ksrsigner /media/KSR/KSK33-1-E_to_D/ksr-root-2018-q3-1-e_to_d.xml (at Wed Ap
r 11 18:36:07 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
```

```
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-1-E_to_D/ksr-root-2018-q3-1-e_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
9949389F5C69E76DC0CEC8A92B75A8BB7E5423FBF03A8BE800ECF59F2CE44367
>> prowler dinosaur classic opulent escape guitarist transit hazardous slowdown sardon
ic spaniel passenger briefcase impartial retouch publisher locale equation blowtorch W
ichita unearth corrosion obtuse typewriter aardvark unicorn vapor opulent Burbank trad
ition crucial graduate <<
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/KSK33-1-E_to_D/skr-root-2018-q3-1-e_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
13DEF14FDF19C450A791AE6319A4F1C4A5DED3E978C43F55CA754CE543B57AD7
>> Aztec telephone unwind document talon bottomless snowslide embezzle repay miracle r
obust Galveston bedlamp Pandora unwind reproduce reindeer telephone stapler ultimate i
sland reproduce cowbell equipment spellbind impartial drainage travesty crucial positi
ve keyboard stethoscope <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180411-183607.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksr\007s\007igner /media
/KSR/KSK33-2-D_to_D/ksr-root-2018-q3-2-d_
Starting: ksrsigner /media/KSR/KSK33-2-D_to_D/ksr-root-2018-q3-2-d_to_d.xml (at Wed Ap
r 11 18:38:14 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
```

```
7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570          20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570    20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-2-D_to_D/ksr-root-2018-q3-2-d_to_d.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
12E17CECD65AE156955C71BF3B002983DC1D47EC533AAB73BAD0769EF96656EB
>> atlas tolerance kiwi unicorn stockman existence tempest escapade preclude fascinate
 hamlet rebellion clockwork adroitness breakup Jamaica sweatband breakaway dashboard u
nicorn dwelling corrosion rhythm hurricane shadow savagery inverse onlooker waffle gos
samer egghead underfoot <<
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/KSK33-2-D_to_D/skr-root-2018-q3-2-d_to_d.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         20326(Klajeyz)/P,19036(Kjqmt
7v)/S
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   20326(Klajeyz)/P,19036(Kjqmt
7v)/S

SHA256 hash of SKR:
A05918310598659DA6B48265386CDA27B904D9676F1D749E48E3AD41A10E24E1
>> ragtime examine beaming company adult narrative fracture Ohio rematch politeness mi
ser glossary classic handiwork surmount celebrate sentence alkali sugar graduate greml
in breakaway indoors onlooker deadbolt torpedo ringbolt decadence ratchet Atlantic blu
ebird tolerance <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180411-183814.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ksrs\007igner /d%033[K
\033[Kmke%033[K033[K033[Kedia/KSR/KSR\007-\007033[K033[K033[KSK\00733-3-C_to_C/ksr-roo
t-2018-q3-3-c_
Starting: ksrsigner /media/KSR/KSK33-3-C_to_C/ksr-root-2018-q3-3-c_to_c.xml (at Wed Ap
r 11 18:40:01 2018 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:            ICANNKSK
    ManufacturerID:   AEP Networks
    Model:            Keyper 9860-2
    Serial:           H1403032

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-04-01T00:00:00 2018-04-22T00:00:00  39570,41824   20326(Klajeyz)/P,19036(Kjqmt
7v)/S
2  2018-04-11T00:00:00 2018-05-02T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
3  2018-04-21T00:00:00 2018-05-12T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
4  2018-05-01T00:00:00 2018-05-22T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
5  2018-05-11T00:00:00 2018-06-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
6  2018-05-21T00:00:00 2018-06-11T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
7  2018-05-31T00:00:00 2018-06-21T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
8  2018-06-10T00:00:00 2018-07-01T00:00:00  39570         20326(Klajeyz)/S,19036(Kjqmt
7v)/P
9  2018-06-20T00:00:00 2018-07-11T00:00:00  41656,39570   20326(Klajeyz)/S,19036(Kjqmt
7v)/P
...VALIDATED.

Validate and Process KSR /media/KSR/KSK33-3-C_to_C/ksr-root-2018-q3-3-c_to_c.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  39570,41656
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656
```

```
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
65318A02B85022AEE8596355858FA560ADD41C9CEAAFDEE1F0A81EFA86B2C553
>> fracture company Oakland aftermath select embezzle blockade performance trauma exam
ine flatfoot equipment music midsummer reindeer fortitude ringbolt souvenir befriend O
ctober Trojan pharmacy tactics tolerance unearth paramount berserk whimsical necklace
pioneer solo enterprise <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2010)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 19036(Kjqmt7v)/S
2 19036(Kjqmt7v)/S
3 19036(Kjqmt7v)/S
4 19036(Kjqmt7v)/S
5 19036(Kjqmt7v)/S
6 19036(Kjqmt7v)/S
7 19036(Kjqmt7v)/S
8 19036(Kjqmt7v)/S
9 19036(Kjqmt7v)/S
Generated new SKR in /media/KSR/KSK33-3-C_to_C/skr-root-2018-q3-3-c_to_c.xml
#  Inception           Expiration           ZSK Tags      KSK Tag(CKA_LABEL)
1  2018-07-01T00:00:00 2018-07-22T00:00:00  41656,39570   19036(Kjqmt7v)/S
2  2018-07-11T00:00:00 2018-08-01T00:00:00  41656         19036(Kjqmt7v)/S
3  2018-07-21T00:00:00 2018-08-11T00:00:00  41656         19036(Kjqmt7v)/S
4  2018-07-31T00:00:00 2018-08-21T00:00:00  41656         19036(Kjqmt7v)/S
5  2018-08-10T00:00:00 2018-08-31T00:00:00  41656         19036(Kjqmt7v)/S
6  2018-08-20T00:00:00 2018-09-10T00:00:00  41656         19036(Kjqmt7v)/S
7  2018-08-30T00:00:00 2018-09-20T00:00:00  41656         19036(Kjqmt7v)/S
8  2018-09-09T00:00:00 2018-09-30T00:00:00  41656         19036(Kjqmt7v)/S
9  2018-09-19T00:00:00 2018-10-10T00:00:00  41656,02134   19036(Kjqmt7v)/S

SHA256 hash of SKR:
BEB2EFF282CFCC589D103D35FB2706BA7C8B04EA2A58BC05B319292DC486A5F1
>> skydive pioneer uncut vagabond miser Saturday spigot everyday quadrant autopsy comm
ence conformist watchword celebrate afflict puberty kiwi Medusa adrift undaunted brick
yard everyday showgirl almighty scallion bottomless breakup clergyman snowslide letter
head reindeer vacancy <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0

********** Log output in ./ksrsigner-20180411-184001.log **********
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# for i in $(ls -l ksr\007
033[[illegible]033[C\033[C\033[C\033[C\033[C\033[C\033[C\033[C\033
[illegible]033[C\033[C\033[C\033[C\033[C\033[C.log); do printlog $
[ 1 pages * 15 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 15 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 15 copy ] sent to printer
2 lines were wrapped
[ 1 pages * 15 copy ] sent to printer
2 lines were wrapped
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# cp -pR /media/KSR/* .
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -kl033[K033[KltrR /me
dia/KSR
```

```
\033[00m/media/KSR:
total 16
drwxr-xr-x 2 root root 4096 Apr 11 18:35 \033[00;34mKSK33-0-D_to_E\033[00m
drwxr-xr-x 2 root root 4096 Apr 11 18:37 \033[00;34mKSK33-1-E_to_D\033[00m
drwxr-xr-x 2 root root 4096 Apr 11 18:39 \033[00;34mKSK33-2-D_to_D\033[00m
drwxr-xr-x 2 root root 4096 Apr 11 18:41 \033[00;34mKSK33-3-C_to_C\033[00m

/media/KSR/KSK33-0-D_to_E:
total 108
-rwxr-xr-x 1 root root 24928 Apr  4 22:27 \033[00;32mskr.xml.20180411183203\033[00m
-rwxr-xr-x 1 root root 19554 Apr  4 22:27 \033[00;32mksr-root-2018-q3-0-d_to_e.xml\033
[00m
-rwxr-xr-x 1 root root  1344 Apr  4 22:27 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Apr 11 18:35 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Apr 11 18:35 \033[00;32mskr-root-2018-q3-0-d_to_e.xml\033
[00m

/media/KSR/KSK33-1-E_to_D:
total 108
-rwxr-xr-x 1 root root 24928 Apr  4 22:27 \033[00;32mskr.xml.20180411183607\033[00m
-rwxr-xr-x 1 root root 19554 Apr  4 22:27 \033[00;32mksr-root-2018-q3-1-e_to_d.xml\033
[00m
-rwxr-xr-x 1 root root  1344 Apr  4 22:27 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Apr 11 18:37 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Apr 11 18:37 \033[00;32mskr-root-2018-q3-1-e_to_d.xml\033
[00m

/media/KSR/KSK33-2-D_to_D:
total 108
-rwxr-xr-x 1 root root 24928 Apr  4 22:27 \033[00;32mskr.xml.20180411183814\033[00m
-rwxr-xr-x 1 root root 19554 Apr  4 22:27 \033[00;32mksr-root-2018-q3-2-d_to_d.xml\033
[00m
-rwxr-xr-x 1 root root  1344 Apr  4 22:27 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 24928 Apr 11 18:39 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 24928 Apr 11 18:39 \033[00;32mskr-root-2018-q3-2-d_to_d.xml\033
[00m

/media/KSR/KSK33-3-C_to_C:
total 92
-rwxr-xr-x 1 root root 24928 Apr  4 22:27 \033[00;32mskr.xml.20180411184001\033[00m
-rwxr-xr-x 1 root root 19554 Apr  4 22:27 \033[00;32mksr-root-2018-q3-3-c_to_c.xml\033
[00m
-rwxr-xr-x 1 root root  1148 Apr  4 22:27 \033[00;32mkskschedule.json\033[00m
-rwxr-xr-x 1 root root 20347 Apr 11 18:41 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root 20347 Apr 11 18:41 \033[00;32mskr-root-2018-q3-3-c_to_c.xml\033
[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# sync
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# umount /media/KSR
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]#
\033[00mtotal 2064
-rwxr-xr-x 1 root root  15547 Jun  9  2010 \033[00;32mksr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root  40555 Jun  9  2010 \033[00;32mwksr-20100517-172720.log\033[00m
-rwxr-xr-x 1 root root    190 Jun 16  2010 \033[00;32mKSKSlotDB.config.db\033[00m
-rwxr-xr-x 1 root root   2668 Jun 16  2010 \033[00;32mkskgen-20100616-211906.log\033[0
0m
-rwxr-xr-x 1 root root    765 Jun 16  2010 \033[00;32mKjqmt7v.csr\033[00m
-rwxr-xr-x 1 root root  36864 Jun 16  2010 \033[00;32mttyaudit-ttyUSB1-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root  45056 Jun 16  2010 \033[00;32mttyaudit-ttyUSB0-20100616-182157
.log\033[00m
-rwxr-xr-x 1 root root  18364 Jun 16  2010 \033[00;32mskr-root-2010-q3-2.xml\033[00m
-rwxr-xr-x 1 root root   4473 Jun 16  2010 \033[00;32mksrsigner-20100616-214329.log
```

```
\033[00m
-rwxr-xr-x 1 root root 196608 Jun 16  2010 \033[00;32mscript-20100616.log\033[00m
-rwxr-xr-x 1 root root   7674 Jun 16  2010 \033[00;32mscript-20100616-2209utc.log\033[
00m
-rwxr-xr-x 1 root root  18364 Oct 31  2010 \033[00;32mskr.xml.20101101181303\033[00m
-rwxr-xr-x 1 root root  15547 Oct 31  2010 \033[00;32mksr-root-2011-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  18402 Nov  1  2010 \033[00;32mskr-root-2011-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5504 Nov  1  2010 \033[00;32mksrsigner-20101101-181303.log
\033[00m
-rwxr-xr-x 1 root root  14005 Nov  1  2010 \033[00;32mttyaudit-ttyUSB0-20101101-175457
.log\033[00m
-rwxr-xr-x 1 root root   7161 Nov  1  2010 \033[00;32mscript-20101101.log\033[00m
-rwxr-xr-x 1 root root  18402 Feb  7  2011 \033[00;32mskr.xml.20110511181632\033[00m
-rwxr-xr-x 1 root root  15547 Apr 25  2011 \033[00;32mksr-root-2011-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   1400 May 11  2011 \033[00;32mksrsigner-20110511-181351.log
\033[00m
-rwxr-xr-x 1 root root  18402 May 11  2011 \033[00;32mskr-root-2011-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   5510 May 11  2011 \033[00;32mksrsigner-20110511-181632.log
\033[00m
-rwxr-xr-x 1 root root  14374 May 11  2011 \033[00;32mttyaudit-ttyUSB0-20110511-180559
.log\033[00m
-rwxr-xr-x 1 root root   9133 May 11  2011 \033[00;32mscript-20110511.log\033[00m
-rwxr-xr-x 1 root root  18404 Jul 20  2011 \033[00;32mskr.xml.20110930181607\033[00m
-rwxr-xr-x 1 root root  15587 Sep 23  2011 \033[00;32mksr-root-2012-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  18422 Sep 30  2011 \033[00;32mskr-root-2012-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5609 Sep 30  2011 \033[00;32mksrsigner-20110930-181607.log
\033[00m
-rwxr-xr-x 1 root root  12034 Sep 30  2011 \033[00;32mttyaudit-ttyUSB0-20110930-180703
.log\033[00m
-rwxr-xr-x 1 root root   7270 Sep 30  2011 \033[00;32mscript-20110930.log\033[00m
-rwxr-xr-x 1 root root  18424 Feb  2  2012 \033[00;32mskr.xml.20120522151741\033[00m
-rwxr-xr-x 1 root root  15571 May  9  2012 \033[00;32mksr-root-2012-q3-0.xml\033[00m
-rwxr-xr-x 1 root root  18414 May 22  2012 \033[00;32mskr-root-2012-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   5528 May 22  2012 \033[00;32mksrsigner-20120522-151741.log
\033[00m
-rwxr-xr-x 1 root root  12034 May 22  2012 \033[00;32mttyaudit-ttyUSB0-20120522-150621
.log\033[00m
-rwxr-xr-x 1 root root  13817 May 22  2012 \033[00;32mscript-20120522.log\033[00m
-rwxr-xr-x 1 root root  18324 Jul 26  2012 \033[00;32mskr.xml.20121112155152\033[00m
-rwxr-xr-x 1 root root  15371 Oct 12  2012 \033[00;32mksr-root-2013-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  18314 Nov 12  2012 \033[00;32mskr-root-2013-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5529 Nov 12  2012 \033[00;32mksrsigner-20121112-155152.log
\033[00m
-rwxr-xr-x 1 root root  12044 Nov 12  2012 \033[00;32mttyaudit-ttyUSB0-20121112-154229
.log\033[00m
-rwxr-xr-x 1 root root  12249 Nov 12  2012 \033[00;32mscript-20121112.log\033[00m
-rwxr-xr-x 1 root root  18314 Feb 12  2013 \033[00;32mskr.xml.20130502190633\033[00m
-rwxr-xr-x 1 root root  15371 Apr  5  2013 \033[00;32mksr-root-2013-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   4004 May  2  2013 \033[00;32mksrsigner-20130502-190252.log
\033[00m
-rwxr-xr-x 1 root root  18314 May  2  2013 \033[00;32mskr-root-2013-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   5502 May  2  2013 \033[00;32mksrsigner-20130502-190633.log
\033[00m
-rwxr-xr-x 1 root root  12397 May  2  2013 \033[00;32mttyaudit-ttyUSB0-20130502-185222
.log\033[00m
-rwxr-xr-x 1 root root  21494 May  2  2013 \033[00;32mscript-20130502.log\033[00m
-rwxr-xr-x 1 root root  18314 Aug  7  2013 \033[00;32mskr.xml.20131024184618\033[00m
-rwxr-xr-x 1 root root  15371 Oct  4  2013 \033[00;32mksr-root-2014-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  18314 Oct 24  2013 \033[00;32mskr-root-2014-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5512 Oct 24  2013 \033[00;32mksrsigner-20131024-184618.log
\033[00m
-rwxr-xr-x 1 root root  12044 Oct 24  2013 \033[00;32mttyaudit-ttyUSB0-20131024-182843
.log\033[00m
-rwxr-xr-x 1 root root   9167 Oct 24  2013 \033[00;32mscript-20131024.log\033[00m
-rwxr-xr-x 1 root root  18314 Feb 13  2014 \033[00;32mskr.xml.20140417183604\033[00m
-rwxr-xr-x 1 root root  15353 Apr  3  2014 \033[00;32mksr-root-2014-q3-0.xml\033[00m
-rwxr-xr-x 1 root root  18314 Apr 17  2014 \033[00;32mskr-root-2014-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   5511 Apr 17  2014 \033[00;32mksrsigner-20140417-183604.log
\033[00m
-rwxr-xr-x 1 root root  12034 Apr 17  2014 \033[00;32mttyaudit-ttyUSB0-20140417-182117
.log\033[00m
-rwxr-xr-x 1 root root   5853 Apr 17  2014 \033[00;32mscript-20140417.log\033[00m
-rwxr-xr-x 1 root root  18314 Nov 10  2014 \033[00;32mskr.xml.20141120201132\033[00m
-rwxr-xr-x 1 root root  15371 Nov 10  2014 \033[00;32mksr-root-2015-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  18314 Nov 20  2014 \033[00;32mskr-root-2015-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5490 Nov 20  2014 \033[00;32mksrsigner-20141120-201132.log
\033[00m
-rwxr-xr-x 1 root root  12042 Nov 20  2014 \033[00;32mttyaudit-ttyUSB0-20141120-200407
.log\033[00m
-rwxr-xr-x 1 root root   5462 Nov 20  2014 \033[00;32mscript-20141120-1.log\033[00m
-rwxr-xr-x 1 root root  15353 Apr  1  2015 \033[00;32mksr-root-2015-q3-0.xml\033[00m
-rwxr-xr-x 1 root root  18314 Apr  1  2015 \033[00;32mskr.xml.20150409183038\033[00m
-rwxr-xr-x 1 root root  18314 Apr  9  2015 \033[00;32mskr-root-2015-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   5621 Apr  9  2015 \033[00;32mksrsigner-20150409-183038.log
\033[00m
-rwxr-xr-x 1 root root  15774 Apr  9  2015 \033[00;32mttyaudit-ttyUSB0-20150409-180743
.log\033[00m
-rwxr-xr-x 1 root root   5636 Apr  9  2015 \033[00;32mksrsigner-20150409-193635.log
\033[00m
-rwxr-xr-x 1 root root  33966 Apr  9  2015 \033[00;32mttyaudit-ttyUSB0-20150409-190117
.log\033[00m
-rwxr-xr-x 1 root root   5636 Apr  9  2015 \033[00;32mksrsigner-20150409-205227.log
\033[00m
-rwxr-xr-x 1 root root  34895 Apr  9  2015 \033[00;32mttyaudit-ttyUSB0-20150409-202837
.log\033[00m
-rwxr-xr-x 1 root root  19175 Apr  9  2015 \033[00;32mscript-20150409.log\033[00m
-rwxr-xr-x 1 root root  18314 Nov  4  2015 \033[00;32mskr.xml.20151112193232\033[00m
-rwxr-xr-x 1 root root  15371 Nov  4  2015 \033[00;32mksr-root-2016-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  18314 Nov 12  2015 \033[00;32mskr-root-2016-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5547 Nov 12  2015 \033[00;32mksrsigner-20151112-193232.log
\033[00m
-rwxr-xr-x 1 root root  12215 Nov 12  2015 \033[00;32mttyaudit-ttyUSB0-20151112-191111
.log\033[00m
-rwxr-xr-x 1 root root   7282 Nov 12  2015 \033[00;32mscript-20151112.log\033[00m
-rwxr-xr-x 1 root root  18314 Apr 29  2016 \033[00;32mskr.xml.20160512192325\033[00m
-rwxr-xr-x 1 root root  14301 Apr 29  2016 \033[00;32mksr-root-2016-q3-fallback-1.xml
\033[00m
-rwxr-xr-x 1 root root  18314 Apr 29  2016 \033[00;32mskr.xml.20160512190619\033[00m
-rwxr-xr-x 1 root root  15994 Apr 29  2016 \033[00;32mskr-root-2016-q3-0.xml\033[00m
-rwxr-xr-x 1 root root  18599 May 12  2016 \033[00;32mskr-root-2016-q3-0.xml\033[00m
-rwxr-xr-x 1 root root   5534 May 12  2016 \033[00;32mksrsigner-20160512-190619.log
\033[00m
-rwxr-xr-x 1 root root  17908 May 12  2016 \033[00;32mskr-root-2016-q3-fallback-1.xml
\033[00m
-rwxr-xr-x 1 root root   5566 May 12  2016 \033[00;32mksrsigner-20160512-192325.log
\033[00m
-rwxr-xr-x 1 root root  12484 May 12  2016 \033[00;32mttyaudit-ttyUSB0-20160512-184752
.log\033[00m
-rwxr-xr-x 1 root root  15870 May 12  2016 \033[00;32mscript-20160512.log\033[00m
-rwxr-xr-x 1 root root  19557 Oct 24  2016 \033[00;32mksr-root-2017-q1-0.xml\033[00m
-rwxr-xr-x 1 root root  21083 Oct 24  2016 \033[00;32mskr.xml.20161027183803\033[00m
-rwxr-xr-x 1 root root  20348 Oct 27  2016 \033[00;32mskr.xml\033[00m
-rwxr-xr-x 1 root root  20348 Oct 27  2016 \033[00;32mskr-root-2017-q1-0.xml\033[00m
-rwxr-xr-x 1 root root   5501 Oct 27  2016 \033[00;32mksrsigner-20161027-183803.log
```

```
\033[00m
-rwxr-xr-x 1 root root   2974 Oct 27  2016 \033[00;32mKSKSlotDB.db\033[00m
-rwxr-xr-x 1 root root   2712 Oct 27  2016 \033[00;32mkskgen-20161027-184920.log\033[0
0m
-rwxr-xr-x 1 root root    817 Oct 27  2016 \033[00;32mKlajeyz.csr\033[00m
-rwxr-xr-x 1 root root    357 Oct 27  2016 \033[00;32mkeybackup-20161027-185705.log
\033[00m
-rwxr-xr-x 1 root root    357 Oct 27  2016 \033[00;32mkeybackup-20161027-200501.log
\033[00m
-rwxr-xr-x 1 root root  28791 Oct 27  2016 \033[00;32mttyaudit-ttyUSB0-20161027-182428
.log\033[00m
-rwxr-xr-x 1 root root  33568 Oct 27  2016 \033[00;32mttyaudit-ttyUSB0-20161027-202240
.log\033[00m
-rwxr-xr-x 1 root root  17803 Oct 27  2016 \033[00;32mscript-20161027.log\033[00m
-rwxr-xr-x 1 root root   6505 Apr 27  2017 \033[00;32mksrsigner-20170427-183853.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 27  2017 \033[00;34mKSK29-0-C_to_D\033[00m
-rwxr-xr-x 1 root root   6228 Apr 27  2017 \033[00;32mksrsigner-20170427-184519.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 27  2017 \033[00;34mKSK29-1-D_to_C\033[00m
-rwxr-xr-x 1 root root   6224 Apr 27  2017 \033[00;32mksrsigner-20170427-184912.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 27  2017 \033[00;34mKSK29-2-C_to_C\033[00m
-rwxr-xr-x 1 root root  12913 Apr 27  2017 \033[00;32mttyaudit-ttyUSB0-20170427-182024
.log\033[00m
-rwxr-xr-x 1 root root  16683 Apr 27  2017 \033[00;32mscript-20170427.log\033[00m
-rwxr-xr-x 1 root root      0 Oct 18 17:46 \033[00;32mscript-20171018.log\033[00m
-rwxr-xr-x 1 root root   8192 Oct 18 17:48 \033[00;32mttyaudit-ttyUSB0-20171018-174745
.log\033[00m
-rwxr-xr-x 1 root root   6681 Oct 18 18:25 \033[00;32mksrsigner-20171018-181941.log
\033[00m
drwxr-xr-x 2 root root   4096 Oct 18 18:25 \033[00;34mKSK31-0-D_to_E\033[00m
-rwxr-xr-x 1 root root   6698 Oct 18 18:31 \033[00;32mksrsigner-20171018-182803.log
\033[00m
drwxr-xr-x 2 root root   4096 Oct 18 18:31 \033[00;34mKSK31-1-E_to_D\033[00m
-rwxr-xr-x 1 root root   6678 Oct 18 18:34 \033[00;32mksrsigner-20171018-183150.log
\033[00m
drwxr-xr-x 2 root root   4096 Oct 18 18:34 \033[00;34mKSK31-2-D_to_D\033[00m
-rwxr-xr-x 1 root root   6361 Oct 18 18:37 \033[00;32mksrsigner-20171018-183453.log
\033[00m
drwxr-xr-x 2 root root   4096 Oct 18 18:37 \033[00;34mKSK31-3-C_to_C\033[00m
-rwxr-xr-x 1 root root   4384 Oct 18 18:54 \033[00;32mttyaudit-ttyUSB0-20171018-175253
.log\033[00m
-rwxr-xr-x 1 root root  23163 Oct 18 18:54 \033[00;32mscript-20171018-v2.log\033[00m
-rwxr-xr-x 1 root root  10002 Apr 11 18:25 \033[00;32mttyaudit-ttyUSB0-20180411-181102
.log\033[00m
-rwxr-xr-x 1 root root   6775 Apr 11 18:35 \033[00;32mksrsigner-20180411-183203.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 11 18:35 \033[00;34mKSK33-0-D_to_E\033[00m
-rwxr-xr-x 1 root root   6783 Apr 11 18:37 \033[00;32mksrsigner-20180411-183607.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 11 18:37 \033[00;34mKSK33-1-E_to_D\033[00m
-rwxr-xr-x 1 root root   6776 Apr 11 18:39 \033[00;32mksrsigner-20180411-183814.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 11 18:39 \033[00;34mKSK33-2-D_to_D\033[00m
drwxr-xr-x 2 root root   4096 Apr 11 18:41 \033[00;34mtmp\033[00m
-rwxr-xr-x 1 root root  20480 Apr 11 18:41 \033[00;32mscript-20180411.log\033[00m
-rwxr-xr-x 1 root root   6469 Apr 11 18:41 \033[00;32mksrsigner-20180411-184001.log
\033[00m
drwxr-xr-x 2 root root   4096 Apr 11 18:41 \033[00;34mKSK33-3-C_to_C\033[00m
-rwxr-xr-x 1 root root      0 Apr 11 18:58 \033[00;32mttyaudit-ttyUSB0-20180411-185854
.log\033[00m
\033[m\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# ls -ltr | taio\033
[K033[Kl
drwxr-xr-x 2 root root   4096 Apr 11 18:35 KSK33-0-D_to_E
-rwxr-xr-x 1 root root   6783 Apr 11 18:37 ksrsigner-20180411-183607.log
drwxr-xr-x 2 root root   4096 Apr 11 18:37 KSK33-1-E_to_D
-rwxr-xr-x 1 root root   6776 Apr 11 18:39 ksrsigner-20180411-183814.log
drwxr-xr-x 2 root root   4096 Apr 11 18:39 KSK33-2-D_to_D
drwxr-xr-x 2 root root   4096 Apr 11 18:41 tmp
-rwxr-xr-x 1 root root   6469 Apr 11 18:41 ksrsigner-20180411-184001.log
drwxr-xr-x 2 root root   4096 Apr 11 18:41 KSK33-3-C_to_C
-rwxr-xr-x 1 root root      0 Apr 11 18:58 ttyaudit-ttyUSB0-20180411-185854.log
-rwxr-xr-x 1 root root  32768 Apr 11 19:03 script-20180411.log
\033]0;root@localhost:/media/HSMFD\007[root@localhost HSMFD]# exit
exit

Script done on Wed 11 Apr 2018 07:08:41 PM UTC
```

```
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 H1403032 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 BBL CRC32: 0x757574CA
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 H1403032 011403 ABL 011 : Tamper Challenge Response Key
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 ####################################
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 ###     ABL tamper records       ###
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 ####################################
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 ====================================
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 vextoosTamperCount:     0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 vintoosTamperCount:     47
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 vbboosTamperCount:      0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 maxstrtempTamperCount:  0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 minstrtempTamperCount:  0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 meshTamperCount:        0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 extampSMKTamperCount:   0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 extampIMKTamperCount:   0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 tempdiffTamperCount:    0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 pfTamperCount:          47
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 restartTamperCount:     149
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 Current tamper bitmaps:
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 ======================
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
```

```
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:44+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 ========================================
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 Board is P2020RDB
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 board_smp_init: 2 cpu
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:45+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2018-04-11T18:11:45+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0 Starting next program at v0015183c
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0 Starting K-Series Kernel
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0 Copyright AEP Networks Ltd. All Rights Reserved.
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:46+0000        ttyUSB0 Wed Apr 11 17:11:37 2018
2018-04-11T18:11:46+0000        ttyUSB0
2018-04-11T18:11:47+0000        ttyUSB0 Starting auditd v2.0 ... started.
2018-04-11T18:11:47+0000        ttyUSB0
2018-04-11T18:11:47+0000        ttyUSB0 Interface 0 configured for IPv6.
2018-04-11T18:11:47+0000        ttyUSB0
2018-04-11T18:11:47+0000        ttyUSB0 Interface 0 configured for IPv4.
2018-04-11T18:11:47+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0 Starting USB driver...
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0 9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0
2018-04-11T18:11:48+0000        ttyUSB0
```

```
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running DES POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 DES POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running Triple DES POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Triple DES POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running AES POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 AES POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running SHA1 POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 SHA1 POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running SHA2 POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 SHA2 POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running RandomGen POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 RandomGen POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running RSA POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 RSA POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running DSA POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 DSA POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 Running ECC POST Test
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:50+0000        ttyUSB0 ECC POST Test Passed
2018-04-11T18:11:50+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 Audit on 11/4/2018 17:11:40 00100008
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 Keyper 9860-2  Serial Number H1403032
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 Memory Usage:
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 RAM (free/total)        197Mb/256Mb
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0    black store          512b
```

```
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0    statistics           112b
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0    other                116b
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 RedStore (free/total)   109Kb/128Kb
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 Network Configuration:
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 IPv4: enabled
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 IPv6: enabled
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 MAC/IP address(es): 00:E0:06:C0:B2:3D / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b23d/64
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 HSM Port: 05000
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 HSM Gateway(s): 0.0.0.0 ::
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 Software Versions:
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 BBL 010 ABL 011 App 023
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 CPLD Version:
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 1.9
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 SCR Firmware Version:
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 OROS-R2.99-R1.20
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 HmcListener: Created IPv4 socket 10 on port 3000.
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:51+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2018-04-11T18:11:51+0000        ttyUSB0
2018-04-11T18:11:52+0000        ttyUSB0 Audit on 11/4/2018 17:11:41 00100003
2018-04-11T18:11:52+0000        ttyUSB0
```

ROOT DNSSEC SCRIPT EXCEPTION

EXCEPTION:

		INITIALS	TIME
1.	ACT 4 STEP 23 PAGE 19 DATE AND TIME: 2018/4/11 19:27	JD	19:27
2.	NEW TEB # BB51184631 PRE-PREPARED TEB # BB51184644 DID NOT SEAL PROPERLY, SO NEW TEB # BB51184631 WAS CREATED FOR LAPTOP 1. SEALING STRIP WAS DISPOSED OF IN WASTEBASKET.	JD	19:31

Place HSMFDs and OS DVDs into the TEB

Step	Activity	Initials	Time

18	CA unmounts the HSMFD by executing the following commands on the terminal window:
	`cd /tmp`
	`umount /media/HSMFD`
	CA removes the HSMFD, then places it on the holder.
		JD	19:18

19	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, printer, display and network.	JD	19:19
20	CA places 2 HSMFD, 2 OS DVD, 1 paper with printed HSMFD hash into a prepared TEB, then seals it.	JD	19:21
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 20170403 + HSMFD: TEB # BB46584489**	JD	19:22

Distribute the HSMFDs

Step	Activity	Initials	Time
22	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for both RKOS (for SKR exchange with RZM and for process review).	JD	19:22

Return the Laptop to TEB

Step	Activity	Initials	Time
23	CA places the laptop into a prepared TEB, then seals it.	JD	19:31
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. BB51184631 **Laptop1: TEB # ~~BB51184644~~ / Serial # 41593712005**	JD	19:32

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. **CO3: Olaf Kolkman** **OP TEB # BB46584493** **CO4: Robert Seastrom** **OP TEB # BB46584484** **CO5: Christopher Griffiths** **OP TEB # BB46584485** **CO6: Gaurab Upadhaya** **OP TEB # BB46584487** **CO7: Alain Aina** **OP TEB # BB46584488**	JD	19:41

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO3	OP 3 of 7	BB46584493	Olaf Kolkman		2018 April	19:35	JD
CO4	OP 4 of 7	BB46584484	Robert Seastrom		2018 Apr 11	1937	JD
CO5	OP 5 of 7	BB46584485	Christopher Griffiths		2018 Apr 11	1937	JD
CO6	OP 6 of 7	BB46584487	Gaurab Upadhaya		2018 Apr 11	19:39	JD
CO7	OP 7 of 7	BB46584488	Alain Aina		2018 Apr 11	19:41	JD

Return the Equipment to Safe #1

Step	Activity	Initials	Time
26	CA and IW brings a cart and escorts SSC1 into the safe room.	JD	19:42
27	SSC1 opens Safe #1 while shielding the combination from the camera.	JD	19:43
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.**	JD	19:43
29	CA returns each equipment to the Safe by following the steps below: a) CAREFULLY remove the equipment TEB from the cart. b) Read out the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time and signature on the safe log where **"Return"** is indicated. d) IW verifies the safe log entry, then initials it. **HSM3: TEB # BB51184645 / Serial # H1403032** ✓ **Laptop1: TEB # ~~BB51184644~~ (Should) / Serial # 41593712005** / SEE EXCEPTION **OS DVD (release 20170403) + HSMFD: TEB # BB46584489** ✓	JD	19:46

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.	JD	19:47
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.	JD	19:48
32	CA, SSC1 and IW leaves the safe room with the cart, closing the door behind them.	JD	19:48

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.	JD	19:49
34	SSC2 opens Safe #2 while shielding the combination from the camera.	JD	19:50
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.**	JD	19:51

CO Returns the Credentials to Safe #2

Step	Activity	Initials	Time
36	One by one, the selected CO returns the TEBs by following the 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. **CO3: Olaf Kolkman** **Box # 1239** **OP TEB # BB46584493** ✓ **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584484** ✓ **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46584485** ✓ **CO6: Gaurab Upadhaya** **Box # 1261** ✓ **OP TEB # BB46584487** **CO7: Alain Aina** **Box # 1242** **OP TEB # BB46584488** ✓	JD	19:58

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.	JD	19:58
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.	JD	19:59
39	CA, IW, SSC2, and COs leave safe room closing the door behind them.	JD	19:59

Act 5. Close the Key Signing Ceremony

Participants Signing of IW's Script

Step	Activity	Initials	Time
1	CA reads the exceptions that may have occurred during the ceremony.	JD	20:06
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.	JD	20:10
3	CA reviews IW's script, then signs the participants list.	JD	20:12

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.	JD	20:12

Post Ceremony Information

Step	Activity	Initials	Time
5	CA informs onsite participants about post ceremony activities.	JD	20:14

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.	JD	20:23
7	CA notifies the SA to stop the audit camera video recording.	JD	20:23

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: **20171018 00:00:00 to 20180412 00:00:00 UTC** e) IW's attestation (Appendix B). f) SA's attestation (Appendix C and D). All TEBs are labeled **Root DNSSEC KSK Ceremony 33**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	JD	22:26

Appendix A. Audit Bundle Checklist

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

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

A.2. Key Ceremony Script (by IW)

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

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

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

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

Two electronic copies of the following:

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

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

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

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

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

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

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

A.7. Other items

If applicable.

Appendix B. Key Ceremony Script (by IW)

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

IW: JONATHAN DENISON

Signature: 

Date: 2018 Apr 11

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

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

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

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

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

Range: **20171018 00:00:00 to 20180412 00:00:00 UTC.**

SA: Brian Martin

Signature: 

Date: 2018 Apr 11

Appendix D. Firewall Configuration Review (by SA)

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

SA: Reed Quinn

Signature: Reed Quinn

Date: 2018 Apr 11

```
version 12.1X46-D35.1;
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 "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## 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 "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"; ## 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;
        source-address 10.4.29.1;
    }
}
chassis {
    config-button no-rescue no-clear;
}
interfaces {
    interface-range access {
        member-range ge-0/0/0 to ge-0/0/8;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-access;
                }
            }
        }
    }
    interface-range video {
        member-range ge-0/0/9 to ge-0/0/12;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-video;
                }
            }
        }
    }
    interface-range wifi {
        member ge-0/0/13;
        unit 0 {
            family inet {
                address 10.100.1.1/24;
            }
        }
    }
    interface-range guest {
        member ge-0/0/14;
        member ge-0/0/15;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-guest;
                }
            }
        }
    }
    ge-0/0/0 {
        description "Access Control Server";
    }
    ge-0/0/1 {
        description "Access Control Client Custom Solution";
    }
    ge-0/0/2 {
        description "Intrusion Detection Panel";
    }
    ge-0/0/3 {
        description "Environment Monitoring";
    }
    ge-0/0/4 {
        description "Monitoring Server";
    }
    ge-0/0/5 {
        description "IRIS Enrollment";
    }
    ge-0/0/6 {
        description "Iris Scanner T2";
    }
    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;
    }
}
security {
    ike {
        policy ike-policy-KMF {
            pre-shared-key ascii-text XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX "; ## SECRET-DATA
        }
        gateway Gateway-to-KMF-West {
            ike-policy ike-policy-KMF;
            address 192.0.35.202;
            external-interface ge-1/0/0;
        }
    }
    ipsec {
        traceoptions {
            flag all;
        }
        proposal IPSecProposal {
            protocol esp;
            authentication-algorithm hmac-sha-256-128;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 7200;
        }
        policy defaultPolicy {
            perfect-forward-secrecy {
                keys group5;
            }
            proposals IPSecProposal;
        }
        vpn vpn-to-KMF-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;
                }
              }
            }
          }
        }
      }
    }
    firewall {
      family inet {
        filter route-engine-filter {
          term deny-icmp-redirects {
            from {
              protocol icmp;
              icmp-type redirect;
            }
            then {
              discard;
            }
          }
          term allow-icmp {
            from {
              protocol icmp;
              icmp-type [ echo-request echo-reply unreachable time-exceeded ];
            }
            then {
              policer small-bw-limit;
              accept;
            }
          }
          term allow-traceroute {
            from {
```

```
            protocol udp;
            port 33434-33534;
          }
          then {
            policer small-bw-limit;
            accept;
          }
        }
        term allow-dns {
          from {
            source-prefix-list {
              resolver-servers;
            }
            protocol udp;
            source-port domain;
          }
          then {
            policer small-bw-limit;
            accept;
          }
        }
        term allow-ntp {
          from {
            source-prefix-list {
              local-prefixes;
              ntp-servers;
            }
            protocol udp;
            port ntp;
          }
          then {
            policer small-bw-limit;
            accept;
          }
        }
        term allow-establish {
          from {
            protocol tcp;
            tcp-established;
          }
          then accept;
        }
        term allow-ipsec-esp {
          from {
            protocol esp;
          }
          then accept;
        }
        term allow-ipsec-udp {
          from {
            protocol udp;
            port 500;
          }
          then accept;
        }
        term allow-ssh {
          from {
            source-address {
              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;
    }
  }
```