Root DNSSEC KSK Ceremony 40

Saturday February 15, 2020

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

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

Abbreviations

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

Participants

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

Title / Roles	Printed Name	Signature	Date	Time
CA	Gustavo Lozano / ICANN		2020 Feb 16	03:36
IW	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Anand Mishra / ICANN			
CO1	Arbogast Fabian			
CO3	João Damas			
CO7	Subramanian Moonesamy			
~~AUD~~	~~Karen Minh Phan / RSM~~			
AUD	Eylan Jordan Torres / RSM			
SA	Brian Martin / ICANN			
SA	Patrick Tudor / ICANN	TUDOR		
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
~~EW~~	~~George Palmer~~			
SW	Kim DAVIS			

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, and you agree that your personal data will be processed in accordance with the ICANN Privacy Policy available at https://www.icann.org/privacy/policy

Instructions for Root DNSSEC KSK Ceremony

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

Ceremony Guidelines:

- The CA leads the ceremony
- Only CAs, IWs, or SAs can enter and escort other participants into Tier 4 (Key Ceremony Room)
- Dual Occupancy is enforced. IW with CA or SA must remain inside Tier 4 (Key Ceremony Room) if participants are present in the room
- CAs, IWs, or SAs may escort participants out of Tier 4 (Key Ceremony Room) at the CA's discretion only if Tier 5 (Safe Room) is not occupied during the ceremony
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log
- The SA starts filming before the participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step
- CA reads each step aloud prior to its performance
- Upon completion of each step, IW announces the time of completion, records the completion time, and initials their copy of the script
- Ceremony participants who notice a problem or an error during the ceremony should interrupt the ceremony. Ceremony participants agree on a resolution before proceeding
- Questions and suggestions for improvement are welcome and can be discussed at any time or after the ceremony during the ceremony debrief

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

- Verify that the audit cameras are recording and the online video streaming is enabled
- Confirm that all of the ceremony attendees have signed in using the visitor log in Tier 3
- Review emergency evacuation procedures
- Explain the use of personal devices and the purpose of this ceremony
- Verify the time and date so that all entries into the script follow a common time source

The CA and IW will then escort the SSCs and TCRs into Tier 5 (Safe Room) to retrieve the following materials:

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

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.	YG	01:11
2	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2.	YG	01:13
3	CA asks that any first time ceremony participants introduce themselves.	YG.	01:13

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.	YG.	01:14
5	CA explains the use of personal electronic devices during the ceremony.	YG.	01:14
6	CA briefly explains the purpose of the ceremony.	YG.	01:15

Verify the Time and Date

Step	Activity	Initials	Time
7	IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: 16 Feb 2020 01:15 **Note: All entries into this script or any logs should follow this common source of time.**	YG.	01:15

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 1 Step(s): 8 Page(s): 6 Date and Time: 16 Feb 2020 01:17	YG.	01:18
2.	IW describes the exception(s) and action(s) below.	YG.	01:18

External witness George Palmer left the room due to needing to catch a flight.

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
8	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)	YG.	01:20
9	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.**	YG.	01:21
10	Perform the following steps to complete the safe log: a) SSC2 removes 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 and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies the entry then initials it.	YG	01:22

COs Extract the Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
11	COs perform the following steps sequentially to retrieve the required TEBs: a) After the CA operates the guard key in the bottom lock, CO uses their tenant key to operate the top lock and open their safe deposit box. b) CO reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB. c) CO reads aloud the TEB numbers, then verifies their integrity while showing them to the audit camera above. d) CO retains the TEB(s) specified below, then locks the safe deposit box. **Note: The CO's key will remain inserted in their safe deposit box lock when specified below.** e) CO writes the date and time, then signs the safe log where **"Remove"** is indicated. f) IW verifies the completed safe log entries, then initials it. **CO1: Arbogast Fabian** **Box # 1791 (Key shall remain in lock)** **OP TEB # BB46584376 (Retain)** **SO TEB # BB46584377 (Retain)** **CO3: João Damas** **Box # 1071 (Key shall remain in lock)** **OP TEB # BB46592091 (Retain)** **SO TEB # BB46584455 (Retain)** **CO7: Subramanian Moonesamy** **Box # 1792 (Key shall remain in lock)** **OP TEB # BB46584384 (Retain)** **SO TEB # BB46584385 (Retain)**	YG	01:30

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 1 Step(s): 18 Page(s): 7 Date and Time: 16 Feb 2020 01:42	YG.	01:45
2.	IW describes the exception(s) and action(s) below.	YG.	01:46

HSM3 and HSM3 Physical keyboard key were returned to Safe #1 due to destruction of HSM3 not being completed today. (Act 4)

As a result, the SO cards are not used, and therefore remains in the TEB bags. &

Act 5, page 27. Step 23 (i) is skipped as SO cards were not used during the ceremony.

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
12	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry then initials it.	YG.	01:30
13	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	YG.	01:31
14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	YG.	01:32

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
15	CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)	YG.	01:33
16	SSC1 opens Safe #1 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.**	YG.	01:34
17	Perform the following steps to complete the safe log: a) SSC1 removes 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 and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies the entry then initials it.	YG.	01:35

Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
18	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified in 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 # BB51184234 (Place on Cart)** **HSM4: TEB # BB51184236 (Place on Cart)** **HSM5W: TEB # BB51184237 (Check and Return)** **Laptop3: TEB # BB81420125 (Check and Return)** **Laptop4: TEB # BB81420103 (Place on Cart)** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386 (Place on Cart)** **KSK-2017: TEB # BB46584387 (Check and Return)** **HSM3 Physical Keyboard Key: TEB # BB21907221 (Place on Cart)**	YG	01:42

Close Safe #1 (Tier 6, Equipment Safe) Exit Tier 5 (Safe Room)

Step	Activity	Initials	Time
19	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry then initials it.	YGT	01:43
20	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	YG.	01:43
21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	YG	01:44

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 2 Step(s): 1 Page(s): 9 Date and Time: 16 Feb 2020 01:51	YG	01:53
2.	IW describes the exception(s) and action(s) below.	YG.	01:55

The script on page 9 states that HSM4 was last verified on 14 Feb 2020, However, it was actually 16 Feb 2020. This is due to safe lock malfunction and the fixing took longer than expected.

Act 2: Equipment Setup

The CA will set up the equipment by performing the following steps:

- Boot the laptop using the OS DVD (the laptop has no permanent storage device)
- Set up the printer
- Verify the laptop date and time
- Connect the HSMFD
- Start the log sessions
- Power ON the HSM (Tier 7)

Laptop Setup

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the listed equipment: a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM4: TEB # BB51184236 / Serial # H1411006** **Last Verified: KSK40-AC 2020-02-~~14~~ 16** **Laptop4: TEB # BB81420103 / Service Tag # F8SVSG2** **Last Verified: KSK36 2019-02-27** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386** **Last Verified: KSK38 2019-08-14**	YGT.	01:51
2	CA performs the following steps to confirm that no hard drive and battery are in the laptop: a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty.	YGT	01:52
3	CA performs the following steps to boot the laptop: a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into the serial port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Immediately insert the **OS DVD release coen-0.4.0**[1] after the laptop power is switched ON.	YGT	01:57
4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	YGT	01:58

OS DVD Checksum Verification

Step	Activity	Initials	Time
5	CA uses the terminal window to executes the following steps: a) Calculate the SHA-256 hash by executing: `sha2wordlist`[2] `< /dev/sr0` IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.** SHA-256 hash: **8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f** PGP Words: **minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document** **Note: The SHA-256 hash of the OS DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/40**	YG.	02:01

Printer Setup

Step	Activity	Initials	Time
6	CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page: `configure-printer`[3]	YG	02:02

Date Setup

Step	Activity	Initials	Time
7	CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock. If the date/time do not match, perform the following steps: a) Execute `date -s "20200215 HH:MM:00"` to set the time. **where `HH` is two-digit hour, `MM` is two-digit minutes and `00` is zero seconds.** b) Execute `date` to confirm the date/time matches the clock.	YG	02:03

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the **Ceremony 38 HSMFD** into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window.	YG.	02:04
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash`[4] `-c` IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 38 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.** **HSMFD SHA-256 HASH** 2019/08/15 # find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist SHA-256: 94862bfae4991cb5b47ed294dab7d5a03c031b0c1f16acb1b61af65ca905bc85 PGP Words: Pluto letterhead briefcase whimsical tonic nebula befriend positive scenic insurgent standard molecule surmount processor sterling Orlando cobra aggregate beeswax article billiard bodyguard ribcage photograph Scotland Bradbury village fascinate revenge almighty showgirl leprosy	YG.	02:07

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 38** and the sheet of paper with the printed HSMFD hash to RKOS.	YG	02:07

Start the Terminal Session Logging

Step	Activity	Initials	Time
11	CA executes the command below using the terminal window to change the working directory to HSMFD: `cd /media/HSMFD`	YG	02:08
12	CA executes the command below to log activities of the **Commands** terminal window: `script script-20200215.log`	YG	02:08

Start the HSM Activity Logging

Step	Activity	Initials	Time

13	CA performs the following steps using the **HSM Output** terminal window to capture the activity logs of the HSM:
	a) Change the working directory to HSMFD by executing:
	`cd /media/HSMFD`
	b) Set the serial port baud rate by executing:
	`stty -F /dev/ttyS0 115200`
	c) Start logging the serial output by executing:
	`ttyaudit`[5] `/dev/ttyS0`
	Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.
		YG	02:09

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	CA performs the following steps to prepare the HSM: a) Ensure an RJ45 blockout is present in the "MGMT" port of the HSM. Install one if not present. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** d) Scroll the logging screen up and locate the HSM serial number. e) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. **HSM4: Serial # H1411006** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	YG.	02:11

Act 3: Activate HSM (Tier 7) and Generate Signatures

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

- The CA activates the HSM using the TCRs' smartcards
- After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop
- The ksrsigner application uses the private key stored in the HSM to generate the SKR
- Note: The SKR contains the digital signatures of the ZSK slated to be used in the next quarter
- The CA then prints the signer log, backs up the newly created SKR, and deactivates the HSM

TCR Credentials Check

Step	Activity	Initials	Time
1	The CA calls each of the COs listed below sequentially to perform the following steps: a) CO reads aloud the TEB number, then CA inspects it for tamper evidence. b) CO and CA open the TEB, then the CA removes the plastic case containing the card(s). c) CA opens the plastic case, then places the card(s) within on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table. **CO1: Arbogast Fabian** **OP TEB # BB46584376** **SO TEB # BB46584377** **CO3: João Damas** **OP TEB # BB46592091** **SO TEB # BB46584455** **CO7: Subramanian Moonesamy** **OP TEB # BB46584384** **SO TEB # BB46584385**	UG	02:16

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
2	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **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 which cards were used below. Each card is returned to its designated card holder after use. 1st OP card 1 of 7 2nd OP card 3 of 7 3rd OP card 7 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	UG	02:18

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
3	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	YG	02:19
4	CA performs the following steps to test the network connectivity between laptop and HSM: a) Use the **Commands** terminal window b) Test connectivity by executing: `ping hsm`[6] c) Wait for responses, then exit by pressing: `Ctrl + C`	YG	02:19

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 1 KSR.**	YG	02:21

Execute the KSR Signer for KSR 2020 Q2

Step	Activity	Initials	Time
6	CA executes the command below on the terminal window to sign the KSR file: `ksrsigner`[7] `/media/KSR/KSK40/ksr-root-2020-q2-0.xml`	YG	02:21
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.	YG.	02:22

VERISIGN

February 11, 2020

To whom it may concern:

This is a letter of verification of employment for Trevor Davis. Verisign, Inc. has employed Mr. Davis full time from September 29, 2014 until present day as a Manager, Cryptographic Business Operations. His work location is in Verisign's corporate headquarters location at:

12061 Bluemont Way
Reston, VA 20190

Sincerely,

Paul Rowson
Director, HR Business Partners
prowson@verisign.com
T: (703) 948-3481
12601 Bluemont Way
Reston, VA 20190

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

12 February 2020

The SHA256 hash of the 2020 Q2 KSR file is:

ksr-root-2020-q2-0.xml:

6901c570ceecd930eb8a1c5575805927878ac46ed48ad0338f89
b320824ad218

The PGP wordlist for the hash above is:

PGP Words: gazelle adviser solo hesitate spyglass unicorn sugar commando trouble maverick befriend equipment indulge intention endow celebrate Neptune maverick snowslide headwaters steamship maverick stagnate concurrent payday matchmaker scallion butterfat miser direction standard borderline

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 3 Step(s): 14 Page(s): 15 Date and Time: 16 Feb 2010 02:30	YG.	02:30
2.	IW describes the exception(s) and action(s) below.	YG.	02:31

Root Zone Maintainer is not present in the room. therefore the KSR FD was given to RKOS.

The RKOS will publish the SKR file as a part of the normal procedure.

Verify the KSR Hash for KSR 2020 Q2

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 themself in front of the room and provide documents for IW to review off camera for the purpose of authentication. **Note: If the RZM representative is not physically present in the room, write the representative's name and *"Remote Participant"* next to the name on the signature line.** b) IW retains the hash and PGP word list for **KSR 2020 Q2**, and employment verification letter provided by the RZM representative and writes their name on the following line: **Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS outside of the ceremony to be included in the final annotated script and the audit bundle.** Trevor Lewis c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.	YG.	02:25
9	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"**	YG.	02:25
10	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in: `/media/KSR/KSK40/skr-root-2020-q2-0.xml`	YG	02:26

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
11	CA executes the commands below using the terminal window to print the KSR Signer log: a) `lpadmin -p HP -o copies-default=X` **Note: Replace "X" with the amount of copies needed for the participants.** b) `printlog`[8] `ksrsigner-202002*.log`	YG	02:27
12	IW attaches a copy of the required ksrsigner log to their script.	YG	02:27

Back up the Newly Created SKR

Step	Activity	Initials	Time

13	CA executes the following commands using the terminal window:
	a) List the contents of the KSR FD by executing:
	`ls -ltrR /media/KSR`
	b) Copy the contents of the KSR FD to the HSMFD by executing:
	`cp -pR /media/KSR/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD to verify it has been copied successfully by executing:
	`ls -ltrR`
	d) Unmount the KSR FD by executing:
	`umount /media/KSR`
		YG	02:29

14	CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative.	YG.	02:29

```
Starting: ksrsigner /media/KSR/KSK40/ksr-root-2020-q2-0.xml (at Sun Feb 16 02:21:33 2020 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-01-01T00:00:00 2020-01-22T00:00:00 33853,22545   20326(Klajeyz)/S
2  2020-01-11T00:00:00 2020-02-01T00:00:00 33853         20326(Klajeyz)/S
3  2020-01-21T00:00:00 2020-02-11T00:00:00 33853         20326(Klajeyz)/S
4  2020-01-31T00:00:00 2020-02-21T00:00:00 33853         20326(Klajeyz)/S
5  2020-02-10T00:00:00 2020-03-02T00:00:00 33853         20326(Klajeyz)/S
6  2020-02-20T00:00:00 2020-03-12T00:00:00 33853         20326(Klajeyz)/S
7  2020-03-01T00:00:00 2020-03-22T00:00:00 33853         20326(Klajeyz)/S
8  2020-03-11T00:00:00 2020-04-01T00:00:00 33853         20326(Klajeyz)/S
9  2020-03-21T00:00:00 2020-04-11T00:00:00 33853,48903   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK40/ksr-root-2020-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-04-01T00:00:00 2020-04-22T00:00:00 48903,33853
2  2020-04-11T00:00:00 2020-05-02T00:00:00 48903
3  2020-04-21T00:00:00 2020-05-12T00:00:00 48903
4  2020-05-01T00:00:00 2020-05-22T00:00:00 48903
5  2020-05-11T00:00:00 2020-06-01T00:00:00 48903
6  2020-05-21T00:00:00 2020-06-11T00:00:00 48903
7  2020-05-31T00:00:00 2020-06-21T00:00:00 48903
8  2020-06-10T00:00:00 2020-07-01T00:00:00 48903
9  2020-06-20T00:00:00 2020-07-11T00:00:00 46594,48903
...PASSED.

SHA256 hash of KSR:
6901C570CEECD930EB8A1C5575805927878AC46ED48AD0338F89B320824AD218
>> gazelle adviser solo hesitate spyglass unicorn sugar commando trouble maverick befriend equipment indulge intention en
dow celebrate Neptune maverick snowslide headwaters steamship maverick stagnate concurrent payday matchmaker scallion but
terfat miser direction standard borderline <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK40/skr-root-2020-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-04-01T00:00:00 2020-04-22T00:00:00 33853,48903   20326(Klajeyz)/S
2  2020-04-11T00:00:00 2020-05-02T00:00:00 48903         20326(Klajeyz)/S
3  2020-04-21T00:00:00 2020-05-12T00:00:00 48903         20326(Klajeyz)/S
4  2020-05-01T00:00:00 2020-05-22T00:00:00 48903         20326(Klajeyz)/S
5  2020-05-11T00:00:00 2020-06-01T00:00:00 48903         20326(Klajeyz)/S
6  2020-05-21T00:00:00 2020-06-11T00:00:00 48903         20326(Klajeyz)/S
7  2020-05-31T00:00:00 2020-06-21T00:00:00 48903         20326(Klajeyz)/S
8  2020-06-10T00:00:00 2020-07-01T00:00:00 48903         20326(Klajeyz)/S
9  2020-06-20T00:00:00 2020-07-11T00:00:00 46594,48903   20326(Klajeyz)/S

SHA256 hash of SKR:
F18565D0DED68791BF027D3B4E28C83EADDBC1178B54053E8F8DC56395AA62AE
>> unwind leprosy fracture savagery tactics speculate Neptune miracle slingshot aftermath klaxon councilman drifter cellu
lose spaniel cumbersome ringbolt suspicious snapline bookseller obtuse equation adult cumbersome payday microscope solo G
alveston preclude pedigree flagpole performance <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
15	CA utilizes 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"**, press **ENT** to confirm. d) When **"Set Offline?"** is displayed, press **ENT** to confirm. e) When **"Insert Card OP #X?"** is displayed, insert the OP card from the card holder. f) When **"PIN?"** is displayed, enter **"11223344"**, then press **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 which cards were used below. Each card is returned to its designated card holder after use. 1st OP card 1 of 7 2nd OP card 3 of 7 3rd OP card 7 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	YG	02:34

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
16	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. **Note: DO NOT unplug the cable connections on the laptop.**	YG	02:34
17	CA places the HSM into a prepared TEB, then seals it.	YG	02:36
18	CA performs the following steps: a) Read aloud the TEB number and HSM serial number, then show 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 along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM TEB on the cart. **HSM4: TEB # BB51184238 / Serial # H1411006**	YG	02:37

Act 4: Zeroize and Dismantle Hardware Security Module

To conclude its period of service, the retiring HSM will be zeroized and have its critical components removed and securely destroyed.

- CA will generate temporary CO cards
- CA will remove all keys from the HSM
- CA will destroy temporary CO cards
- CA will zeroize the HSM
- CA will intentionally tamper the HSM
- CA will dismantle the HSM and extract its critical components
- CA will place the components into a TEB in preparation for offsite secure destruction

Remove the HSM from TEB and Power On

Step	Activity	Initials	Time
1	CA selects the **HSM Output** terminal window.		
2	CA performs the following steps to prepare the HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. e) Plug the null modem cable into the serial port of the HSM. f) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** g) Scroll the logging screen up and locate the HSM serial number. h) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. **HSM3: TEB # BB51184234 / Serial # H1403033** **Last Verified: KSK40-AC 2020-02-14** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		

Issue Temporary Crypto Officer (CO) Cards

Step	Activity	Initials	Time
3	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are used to issue Crypto Officer (CO) cards a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"1.Issue Cards"**, press **ENT** to confirm. h) Select **"1.Issue CO Cards"**, press **ENT** to confirm. i) When **"Issue CO Cards?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. k) When **"Num Req Cards?"** is displayed, enter **"2"**, then press **ENT**. l) When **"Insert Card #X?"** is displayed, insert the required CO card. m) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. n) When **"Remove Card?"** is displayed, remove the CO card. o) Repeat steps l) to n) for the 2nd CO card. p) When **"CO Cards Issued"** is displayed, press **ENT** to confirm. q) Press **CLR** twice to return to the **"Secured"** menu. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		

List and Delete the KSK(s) present in the HSM

Step	Activity	Initials	Time
4	CA performs the following steps to list the KSK(s) present in the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"2.Key Details"**, press **ENT** to confirm. h) When **"List Keys?"** is displayed, press **ENT**. i) Select **"1.Key Summary"**, press **ENT** to confirm. j) When **"Key Summary?"** is displayed, press **ENT**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
5	CA matches the displayed KSK label(s) in the HSM Output terminal window. **KSK-2017: Klajeyz**		
6	CA performs the following steps to delete the KSK(s) from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"7.Erase App Key"**, press **ENT** to confirm. d) When **"Erase App Keys?"** is displayed, press **ENT** to confirm. e) Select **"1.All Keys"**, press **ENT** to confirm. f) The **Klajeyz** key(s) will be selected in the HSM's display with a visible (*) asterisk. Press **ENT** to confirm. **There is no system confirmation prompt**. g) When **Done** is displayed, press **ENT** to return to the App Key Menu. h) Press **CLR** to return to the Key Mgmt menu.		
7	CA performs the following steps to list the KSK(s) from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. f) Press **CLR** to return to the menu **"Secured"**. CA confirms that **KSK-2017: Klajeyz** has been deleted		

Clear and Destroy CO Cards

Step	Activity	Initials	Time
8	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to clear Crypto Officer (CO) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"4.Clear RoleCard"**, press **ENT** to confirm. h) When **"Clear Card?"** is displayed, press **ENT** to confirm. i) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. j) When **"Insert Card #X?"** is displayed, take the required **CO #X** card from the cardholder, show the **CO #X** card to the audit camera and then insert the **CO #X** card into the HSM's card reader. k) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. l) When **"Remove Card?"** is displayed, remove the CO card. m) Repeat steps j) to l) for the 2nd CO card. n) Press **CLR** to return to the main menu **"Secured"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
9	CA uses the shredder to destroy the cleared CO cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.		

Unsecure and Tamper the HSM

Step	Activity	Initials	Time
10	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to issue Crypto Officer (CO) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"6.HSM Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"5.Unsecure"**, press **ENT** to confirm. h) When **"Unsecure?"** is displayed, then press **ENT**. i) When **"DONE"** is displayed, then press **ENT**. It may take a few minutes for the HSM to restart after the zeroization is complete. The HSM will reboot into the **"Unsecured State"** and after the completion of the HSM self test the display should show **"Important Read Manual"** indicating the HSM is in the initialized state. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # ____ 1st SO card ____ of 7 2nd SO card ____ of 7 3rd SO card ____ of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**		
11	CA performs the following steps to tamper the HSM equipment listed below: a) Using **Tool B**, press and hold the recessed button on the rear panel of the HSM located between the LAN and serial ports (remove the tamper sticker if necessary), then release it after 10 seconds to activate the tampering mechanism. **IMK missing recovery mode** will be displayed on the HSM. b) Turn **OFF** the HSM using the rocker switch on the rear panel. Turn **ON** the HSM with the same switch and wait until the **ALERT** LED light is **ON** and **IMK missing recovery mode** is displayed to verify the tampered state. c) Disconnect the power and serial cables from the HSM.		

Open the HSM Case and Remove the Logic Board from HSM3

Step	Activity	Initials	Time
12	IW reads steps 13 to 16 while the CA dismantles **HSM3: Serial # H1403033**.		
13	CA performs the following steps to access the HSM's critical components: a) Using **Tool A+Bit 2**, remove the two screws which secure the serial port to the rear panel. b) Using **Tool A+Bit 1**, remove the four screws from the rear panel of the case which secure the shell. c) Using **Tool A+Bit 1**, remove the four screws from the bottom of the case which secure the shell. d) Using **Tool C**, slice the tamper stickers on the bottom of the case along the seam with the shell. e) Slide the shell toward the back of the case to remove it and place it in the **HSM Parts** bin on the ceremony table. f) Using **Tool A+Bit 3**, remove the two logic board screws nearest to the front panel which secure the plastic logic board cover. g) Remove the plastic logic board cover and place it in the **HSM Parts** bin on the ceremony table. h) Using **Tool A+Bit 3**, remove the two remaining screws which secure the logic board near the rear panel. i) Detach the four cables from the front of the logic board. Open the latches outward to release each of the ribbon cables. j) Using **Tool A+Bit 4**, remove the nut from the cryptographic module securing the ring terminal of the green/yellow wire and slide the ring terminal off of the threaded stud. k) Detach the cable from each side of the cryptographic module connecting it to the logic board.		
14	CA performs the following steps to remove the logic board and batteries: a) Separate the logic board from the HSM case by pulling the logic board up then toward the front of the case. b) Using **Tool D**, cut and remove the zip ties securing the batteries if they are present, then cut the battery terminals that connect the batteries to the logic board. c) Pry the batteries from the logic board by placing the logic board flat on the table and pulling up on each battery with sufficient force to break the adhesive bond. d) Place the batteries in the **HSM Parts** bin on the ceremony table. e) Place the logic board in the **Critical Parts** bin on the ceremony table.		

Remove Cryptographic Module and Card Reader from HSM3

Step	Activity	Initials	Time
15	CA performs the following steps to remove the cryptographic module: a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the cryptographic module to the case. b) Lift the cryptographic module up to separate it from the case. c) Using **Tool C**, remove both connectors from the cryptographic module as flush with the case as possible. d) Place the cryptographic module in the **Critical Parts** bin, and the connectors in the **HSM Parts** bin on the ceremony table.		
16	CA performs the following steps to remove the front panel and card reader: a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the front panel to the bottom of the case. b) Place the front panel in the **HSM Parts** bin on the ceremony table. c) Using **Tool A+Bit 4**, remove the nut which secures the card reader. d) Using **Tool A+Bit 3**, remove the 3 screws which secure the card reader. e) Lift the card reader up to separate it from the case and place it with the ribbon cable in the **Critical Parts** bin on the ceremony table. f) Place the HSM case in the **HSM Parts** bin on the ceremony table.		

Place the Critical HSM3 parts into a TEB

Step	Activity	Initials	Time
17	CA places the container with the following critical parts into a prepared TEB, then seals it. a) Cryptographic Module b) Logic Board c) Card Reader **Note: The HSM case will not be destroyed.**		
18	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Give RKOS the TEB for destruction. **HSM3: TEB # BB81420120**		

Retire HSM Physical Keyboard Key

Step	Activity	Initials	Time
19	CA performs the following steps to retire the listed HSM Physical Keyboard Key: a) Remove the TEB from the cart. b) Inspect TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB. e) RKOS will take possession of the HSM Physical Keyboard Key and place in its designated area. **HSM3 Physical Keyboard Key: TEB # BB21907221** **Last Verified: AT22 2015-07-20**		

Act 5: Secure Hardware

The CA will secure the ceremony hardware by performing the steps below:

- Back up the HSMFD contents
- Print log information
- Place the equipment and TCR credentials inside of TEBs
- Along with IW, escort SSC1 and equipment cart into Tier 5 (Safe Room) to return equipment to Safe #1
- Along with IW, escort SSC2 and TCRs into Tier 5 (Safe Room) to return TCRs' smartcards to Safe #2.

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
1	CA performs the following steps to stop logging: a) Disconnect the null modem and ethernet cables from the laptop. b) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: i) Press `Ctrl + C` ii) Execute `exit` c) Execute the command below using the **Commands** terminal window to stop logging the terminal session: `exit` **Note: The Commands terminal session window will remain open.**	YG	02:38

Prepare blank FDs and back up the HSMFD Contents

Step	Activity	Initials	Time
2	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: `shopt -s dotglob`	YG	02:39
3	CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content: a) `lpadmin -p HP -o copies-default=2` b) `hsmfd-hash`[4] `-p` **Note: One copy for audit bundle and one copy for HSMFD package.**	YG	02:40
4	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrR`	YG	02:40
5	CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs: `mkdir /media/HSMFD1`	YG	02:41
6	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.	YG	02:41
7	CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: `df`	YG	02:42
8	CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD: a) `umount /dev/sdc1` b) `mkfs.vfat -n HSMFD -I /dev/sdc1` c) `mount /dev/sdc1 /media/HSMFD1` d) `cp -pR * /media/HSMFD1`	YG	02:43
9	CA executes the commands below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy, then unmounts the flash drive before removal: a) `hsmfd-hash`[4] `-m` b) `umount /media/HSMFD1`	YG	02:44
10	CA removes the **HSMFD copy**, then places it on the holder. **Wait for the activity light on the backup HSMFD to stop flashing before removal.**	YG.	02:44
11	CA repeats step 6 to 10 for the 2nd copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	YG	02:45
12	CA repeats step 6 to 10 for the 3rd copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	YG	02:46
13	CA repeats step 6 to 10 for the 4th copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	YG	02:47
14	CA repeats step 6 to 10 for the 5th copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	YG	02:48

HSMFD SHA-256 HASH **2020/02/16**

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

SHA-256:    99170d7962918e5ed1f260addb71c6ddb67d16d007f5f3823f41686ef259c380
PGP Words:  prowler bookseller ancient inertia flagpole miracle orca finicky stairway vagab
ond facial perceptive suspense hideaway southward tambourine Scotland insincere backward sa
vagery ahead visitor upset Istanbul cowbell decadence frighten headwaters uproot examine sn
owcap intention
```

Print Logging Information

Step	Activity	Initials	Time
15	CA executes the following commands using the terminal window to print a copy of the logging information: a) `lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true` b) `enscript -2Gr script-202002*.log` c) `enscript -Gr --font="Courier8" ttyaudit-tty*-202002*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**	YG	02:49

Place HSMFDs and OS DVDs into a TEB

Step	Activity	Initials	Time
16	CA executes the following commands using the terminal window to unmount the HSMFD: a) `cd /tmp` b) `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder.	YG.	02:50
17	CA performs the following steps to switch OFF the laptop and remove the OS DVD: a) Remove the OS DVD from the laptop. b) Turn OFF the laptop by pressing the power button. c) Disconnect all connections from the laptop.	YG.	02:51
18	CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it.	YG	02:52
19	CA performs the following steps to verify the TEB: a) Read aloud 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 along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS DVD TEB on the cart. **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951350**	YG.	02:53
20	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	YG.	02:54

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.	YG.	02:56
22	CA performs the following steps: a) Read aloud 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 along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the laptop TEB on the cart. **Laptop4: TEB # BB81420119 / Service Tag # F8SVSG2**	YG.	02:57

```
Script started on Sun Feb 16 02:08:32 2020
root@coen:/media/HSMFD# ping hsm
PING hsm (192.168.0.2) 56(84) bytes of data.
64 bytes from hsm (192.168.0.2): icmp_seq=1 ttl=255 time=0.713 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.419 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.734 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.561 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3075ms
rtt min/avg/max/mdev = 0.419/0.606/0.734/0.130 ms
root@coen:/media/HSMFD# ksrsigner /media/KSR/KSK40/k\007sr-root-2020-q2-0.xml
Starting: ksrsigner /media/KSR/KSK40/ksr-root-2020-q2-0.xml (at Sun Feb 16 02:21:33 2020
UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glib
c_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.s
o.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:          ICANNKSK
    ManufacturerID: Ultra Electronics AEP Networks
    Model:          Keyper 9860-2
    Serial:         H1411006

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-01-01T00:00:00 2020-01-22T00:00:00  33853,22545   20326(Klajeyz)/S
2  2020-01-11T00:00:00 2020-02-01T00:00:00  33853         20326(Klajeyz)/S
3  2020-01-21T00:00:00 2020-02-11T00:00:00  33853         20326(Klajeyz)/S
4  2020-01-31T00:00:00 2020-02-21T00:00:00  33853         20326(Klajeyz)/S
5  2020-02-10T00:00:00 2020-03-02T00:00:00  33853         20326(Klajeyz)/S
6  2020-02-20T00:00:00 2020-03-12T00:00:00  33853         20326(Klajeyz)/S
7  2020-03-01T00:00:00 2020-03-22T00:00:00  33853         20326(Klajeyz)/S
8  2020-03-11T00:00:00 2020-04-01T00:00:00  33853         20326(Klajeyz)/S
9  2020-03-21T00:00:00 2020-04-11T00:00:00  33853,48903   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK40/ksr-root-2020-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-04-01T00:00:00 2020-04-22T00:00:00  48903,33853
2  2020-04-11T00:00:00 2020-05-02T00:00:00  48903
3  2020-04-21T00:00:00 2020-05-12T00:00:00  48903
4  2020-05-01T00:00:00 2020-05-22T00:00:00  48903
5  2020-05-11T00:00:00 2020-06-01T00:00:00  48903
6  2020-05-21T00:00:00 2020-06-11T00:00:00  48903
7  2020-05-31T00:00:00 2020-06-21T00:00:00  48903
8  2020-06-10T00:00:00 2020-07-01T00:00:00  48903
9  2020-06-20T00:00:00 2020-07-11T00:00:00  46594,48903
...PASSED.

SHA256 hash of KSR:
6901C570CEECD930EB8A1C5575805927878AC46ED48AD0338F89B320824AD218
>> gazelle adviser solo hesitate spyglass unicorn sugar commando trouble maverick befrien
d equipment indulge intention endow celebrate Neptune maverick snowslide headwaters steam
ship maverick stagnate concurrent payday matchmaker scallion butterfat miser direction st
andard borderline <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK40/skr-root-2020-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-04-01T00:00:00 2020-04-22T00:00:00  33853,48903   20326(Klajeyz)/S
2  2020-04-11T00:00:00 2020-05-02T00:00:00  48903         20326(Klajeyz)/S
3  2020-04-21T00:00:00 2020-05-12T00:00:00  48903         20326(Klajeyz)/S
4  2020-05-01T00:00:00 2020-05-22T00:00:00  48903         20326(Klajeyz)/S
5  2020-05-11T00:00:00 2020-06-01T00:00:00  48903         20326(Klajeyz)/S
6  2020-05-21T00:00:00 2020-06-11T00:00:00  48903         20326(Klajeyz)/S
7  2020-05-31T00:00:00 2020-06-21T00:00:00  48903         20326(Klajeyz)/S
8  2020-06-10T00:00:00 2020-07-01T00:00:00  48903         20326(Klajeyz)/S
9  2020-06-20T00:00:00 2020-07-11T00:00:00  46594,48903   20326(Klajeyz)/S

SHA256 hash of SKR:
F18565D0DED68791BF027D3B4E28C83EADDBC1178B54053E8F8DC56395AA62AE
>> unwind leprosy fracture savagery tactics speculate Neptune miracle slingshot aftermath
 klaxon councilman drifter cellulose spaniel cumbersome ringbolt suspicious snapline book
seller obtuse equation adult cumbersome payday microscope solo Galveston preclude pedigre
e flagpole performance <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20200216-022133.log **********
root@coen:/media/HSMFD# lp\007admin -p HP -o copies-default=8
root@coen:/media/HSMFD# printlog ksr\007si007gner-20200216-022133.log
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /m\007edia/KSR/
/media/KSR/:
total 16
drwxr-xr-x 2 root root 16384 Feb 16 02:25 \033[0m\033[01;34mKSK40\033[0m

/media/KSR/KSK40:
total 144
-rw-r--r-- 1 root root 20369 Feb  4 23:14 skr.xml.20200216022133
-rw-r--r-- 1 root root 19600 Feb  4 23:14 ksr-root-2020-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb  4 23:14 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16 02:25 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16 02:25 skr-root-2020-q2-0.xml
root@coen:/media/HSMFD# cp -pR /media/Ks\007SR/* .
root@coen:/media/HSMFD# ls -ltrR
.:
total 2992
-rw-r--r-- 1 root root  15547 Jun  9  2010 ksr-root-2010-q3-2.xml
-rw-r--r-- 1 root root  40555 Jun  9  2010 wksr-20100517-172720.log
-rw-r--r-- 1 root root    190 Jun 16  2010 KSKSlotDB.config.db
-rw-r--r-- 1 root root   2668 Jun 16  2010 kskgen-20100616-211906.log
-rw-r--r-- 1 root root    765 Jun 16  2010 Kjqmt7v.csr
-rw-r--r-- 1 root root  36864 Jun 16  2010 ttyaudit-ttyUSB1-20100616-182157.log
-rw-r--r-- 1 root root  45056 Jun 16  2010 ttyaudit-ttyUSB0-20100616-182157.log
-rw-r--r-- 1 root root  18364 Jun 16  2010 skr-root-2010-q3-2.xml
-rw-r--r-- 1 root root   4473 Jun 16  2010 ksrsigner-20100616-214329.log
-rw-r--r-- 1 root root 196608 Jun 16  2010 script-20100616.log
```

```
-rw-r--r-- 1 root root   4096 Jun 16  2010 script-20100616-2209utc.log
-rw-r--r-- 1 root root  15547 Jul  8  2010 wksr_1_20100708144111_14165_198.41.3.50_ksr-ro
ot-2010-q4-1.xml
-rw-r--r-- 1 root root  30915 Jul  8  2010 wksr-20100708-144111.log
-rw-r--r-- 1 root root  15547 Jul  8  2010 ksr-root-2010-q4-1.xml
-rw-r--r-- 1 root root   1400 Jul 12  2010 ksrsigner-20100712-224252.log
-rw-r--r-- 1 root root  18364 Jul 12  2010 skr.xml.20100712224426
-rw-r--r-- 1 root root  18364 Jul 12  2010 skr-root-2010-q4-1.xml
-rw-r--r-- 1 root root   5506 Jul 12  2010 ksrsigner-20100712-224426.log
-rw-r--r-- 1 root root  36885 Jul 12  2010 ttyaudit-ttyUSB0-20100712-212549.log
-rw-r--r-- 1 root root  38221 Jul 12  2010 ttyaudit-ttyUSB1-20100712-212549.log
-rw-r--r-- 1 root root  12956 Jul 12  2010 script-20100712.log
-rw-r--r-- 1 root root  18402 Nov  1  2010 skr.xml.20110207223256
-rw-r--r-- 1 root root  15547 Jan  2  2011 ksr-root-2011-q2-0.xml
-rw-r--r-- 1 root root    188 Feb  7  2011 ksrsigner-20110207-223245.log
-rw-r--r-- 1 root root  18402 Feb  7  2011 skr-root-2011-q2-0.xml
-rw-r--r-- 1 root root   5524 Feb  7  2011 ksrsigner-20110207-223256.log
-rw-r--r-- 1 root root  13997 Feb  7  2011 ttyaudit-ttyUSB0-20110207-221818.log
-rw-r--r-- 1 root root  20709 Feb  7  2011 script-20110207.log
-rw-r--r-- 1 root root  18402 May 11  2011 skr.xml.20110720205839
-rw-r--r-- 1 root root  15551 Jul 19  2011 ksr-root-2011-q4-0.xml
-rw-r--r-- 1 root root  18404 Jul 20  2011 skr-root-2011-q4-0.xml
-rw-r--r-- 1 root root   5508 Jul 20  2011 ksrsigner-20110720-205839.log
-rw-r--r-- 1 root root   8044 Jul 20  2011 ttyaudit-ttyUSB0-20110720-205011.log
-rw-r--r-- 1 root root  32768 Jul 20  2011 script-20110720.log
-rw-r--r-- 1 root root  18422 Sep 30  2011 skr.xml.20120202222928
-rw-r--r-- 1 root root  15591 Jan  9  2012 ksr-root-2012-q2-0.xml
-rw-r--r-- 1 root root  18424 Feb  2  2012 skr-root-2012-q2-0.xml
-rw-r--r-- 1 root root   5509 Feb  2  2012 ksrsigner-20120202-222928.log
-rw-r--r-- 1 root root   8290 Feb  2  2012 ttyaudit-ttyUSB0-20120202-221813.log
-rw-r--r-- 1 root root  42056 Feb  2  2012 script-20120202.log
-rw-r--r-- 1 root root  18414 May 22  2012 skr.xml.20120726185458
-rw-r--r-- 1 root root  15391 Jul  3  2012 ksr-root-2012-q4-0.xml
-rw-r--r-- 1 root root  18324 Jul 26  2012 skr-root-2012-q4-0.xml
-rw-r--r-- 1 root root   5504 Jul 26  2012 ksrsigner-20120726-185458.log
-rw-r--r-- 1 root root  12034 Jul 26  2012 ttyaudit-ttyUSB0-20120726-184435.log
-rw-r--r-- 1 root root   5909 Jul 26  2012 script-20120726.log
-rw-r--r-- 1 root root  18314 Nov 12  2012 skr.xml.20130212222429
-rw-r--r-- 1 root root  15371 Jan 20  2013 ksr-root-2013-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 12  2013 skr-root-2013-q2-0.xml
-rw-r--r-- 1 root root   5506 Feb 12  2013 ksrsigner-20130212-222429.log
-rw-r--r-- 1 root root  12034 Feb 12  2013 ttyaudit-ttyUSB0-20130212-220521.log
-rw-r--r-- 1 root root   8385 Feb 12  2013 script-20130212.log
-rw-r--r-- 1 root root  18314 May  2  2013 skr.xml.20130807214313
-rw-r--r-- 1 root root  15371 Aug  5  2013 ksr-root-2013-q4-0.xml
-rw-r--r-- 1 root root  18314 Aug  7  2013 skr-root-2013-q4-0.xml
-rw-r--r-- 1 root root   5513 Aug  7  2013 ksrsigner-20130807-214313.log
-rw-r--r-- 1 root root   8192 Aug  7  2013 ttyaudit-ttyUSB0-20130807-213355.log
-rw-r--r-- 1 root root   5676 Aug  7  2013 script-20130807.log
-rw-r--r-- 1 root root  18314 Oct 24  2013 skr.xml.20140213225938
-rw-r--r-- 1 root root  15369 Jan 14  2014 ksr-root-2014-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 13  2014 skr-root-2014-q2-0.xml
-rw-r--r-- 1 root root   5513 Feb 13  2014 ksrsigner-20140213-225938.log
-rw-r--r-- 1 root root  12034 Feb 13  2014 ttyaudit-ttyUSB0-20140213-224635.log
-rw-r--r-- 1 root root   5638 Feb 13  2014 script-20140213.log
-rw-r--r-- 1 root root  18314 Apr 17  2014 skr.xml.20140814212827
-rw-r--r-- 1 root root  15369 Jul  7  2014 ksr-root-2014-q4-0.xml
-rw-r--r-- 1 root root      0 Aug 14  2014 ttyaudit-ttyUSB0-20140814-211101.log
-rw-r--r-- 1 root root  18314 Aug 14  2014 skr-root-2014-q4-0.xml
-rw-r--r-- 1 root root   5523 Aug 14  2014 ksrsigner-20140814-212827.log
-rw-r--r-- 1 root root  12032 Aug 14  2014 ttyaudit-ttyUSB0-20140814-211416.log
-rw-r--r-- 1 root root   5563 Aug 14  2014 script-20140814.log
-rw-r--r-- 1 root root  18314 Nov 20  2014 skr.xml.20150122223324
-rw-r--r-- 1 root root  15369 Jan 13  2015 ksr-root-2015-q2-0.xml
-rw-r--r-- 1 root root    762 Jan 13  2015 hash_ksr20.txt
-rw-r--r-- 1 root root  18314 Jan 22  2015 skr-root-2015-q2-0.xml
-rw-r--r-- 1 root root   5526 Jan 22  2015 ksrsigner-20150122-223324.log
-rw-r--r-- 1 root root  12034 Jan 22  2015 ttyaudit-ttyUSB0-20150122-222401.log
-rw-r--r-- 1 root root   5941 Jan 22  2015 script-20150122.log
-rw-r--r-- 1 root root  18314 Jul 28  2015 skr.xml.20150813213057
-rw-r--r-- 1 root root  15369 Jul 28  2015 ksr-root-2015-q4-0.xml
-rw-r--r-- 1 root root  18314 Aug 13  2015 skr-root-2015-q4-0.xml
-rw-r--r-- 1 root root   5505 Aug 13  2015 ksrsigner-20150813-213057.log
-rw-r--r-- 1 root root  17517 Aug 13  2015 ttyaudit-ttyUSB0-20150813-211033.log
-rw-r--r-- 1 root root   5520 Aug 13  2015 ksrsigner-20150814-000517.log
-rw-r--r-- 1 root root  43054 Aug 13  2015 ttyaudit-ttyUSB0-20150813-220137.log
-rw-r--r-- 1 root root   5520 Aug 13  2015 ksrsigner-20150814-002123.log
-rw-r--r-- 1 root root  44497 Aug 13  2015 ttyaudit-ttyUSB1-20150813-220137.log
-rw-r--r-- 1 root root  28755 Aug 13  2015 script-20150813.log
-rw-r--r-- 1 root root  18314 Jan 14  2016 skr.xml.20160211235227
-rw-r--r-- 1 root root  15371 Jan 14  2016 ksr-root-2016-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 11  2016 skr-root-2016-q2-0.xml
-rw-r--r-- 1 root root   5530 Feb 11  2016 ksrsigner-20160211-235227.log
-rw-r--r-- 1 root root  12196 Feb 11  2016 ttyaudit-ttyUSB0-20160211-234001.log
-rw-r--r-- 1 root root   6919 Feb 11  2016 script-20160211.log
-rw-r--r-- 1 root root  17908 May 12  2016 skr.xml.20160811220932
-rw-r--r-- 1 root root  14301 Jul 13  2016 ksr-root-2016-q4-fallback-1.xml
-rw-r--r-- 1 root root  21718 Jul 13  2016 ksr-root-2016-q4-0.xml
-rw-r--r-- 1 root root  18599 Jul 20  2016 skr.xml.20160811215735
-rw-r--r-- 1 root root  21083 Aug 11  2016 skr-root-2016-q4-0.xml
-rw-r--r-- 1 root root   5520 Aug 11  2016 ksrsigner-20160811-215735.log
-rw-r--r-- 1 root root  17908 Aug 11  2016 skr-root-2016-q4-fallback-1.xml
-rw-r--r-- 1 root root   5694 Aug 11  2016 ksrsigner-20160811-220932.log
-rw-r--r-- 1 root root  12499 Aug 11  2016 ttyaudit-ttyUSB0-20160811-213430.log
-rw-r--r-- 1 root root  33540 Aug 11  2016 ttyaudit-ttyUSB0-20160811-222510.log
-rw-r--r-- 1 root root  21200 Aug 11  2016 script-20160811.log
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr.xml.20170202225202
-rw-r--r-- 1 root root  19556 Jan  4  2017 ksr-root-2017-q2-0.xml
-rw-r--r-- 1 root root  20347 Feb  2  2017 skr.xml
-rw-r--r-- 1 root root  20347 Feb  2  2017 skr-root-2017-q2-0.xml
-rw-r--r-- 1 root root   5494 Feb  2  2017 ksrsigner-20170202-225202.log
-rw-r--r-- 1 root root    357 Feb  2  2017 keybackup-20170203-001846.log
-rw-r--r-- 1 root root   2693 Feb  2  2017 kskgen-20170203-001954.log
-rw-r--r-- 1 root root    817 Feb  2  2017 Klajeyz.csr
-rw-r--r-- 1 root root    357 Feb  2  2017 keybackup-20170203-003825.log
-rw-r--r-- 1 root root  48066 Feb  2  2017 ttyaudit-ttyUSB0-20170202-223524.log
-rw-r--r-- 1 root root  23999 Feb  2  2017 script-20170202.log
-rw-r--r-- 1 root root      0 Aug 17  2017 script-20170817.log
-rw-r--r-- 1 root root   8192 Aug 17  2017 ttyaudit-ttyUSB0-20170817-211909.log
-rw-r--r-- 1 root root   6645 Aug 17  2017 ksrsigner-20170817-214009.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[0m\033[01;34mKSK30-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6648 Aug 17  2017 ksrsigner-20170817-214402.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6662 Aug 17  2017 ksrsigner-20170817-214602.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6355 Aug 17  2017 ksrsigner-20170817-214756.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-3-C_to_C\033[0m
-rw-r--r-- 1 root root   2484 Aug 17  2017 ttyaudit-ttyUSB0-20170817-213501.log
-rw-r--r-- 1 root root  65904 Aug 17  2017 script-20170817-2.log
-rw-r--r-- 1 root root   6689 Feb  7  2018 ksrsigner-20180207-224219.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6676 Feb  7  2018 ksrsigner-20180207-224724.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6674 Feb  7  2018 ksrsigner-20180207-224920.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6367 Feb  7  2018 ksrsigner-20180207-225053.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-3-C_to_C\033[0m
-rw-r--r-- 1 root root  13737 Feb  7  2018 ttyaudit-ttyUSB0-20180207-222555.log
```

```
-rw-r--r-- 1 root root  23281 Feb  7  2018 script-20180207.log
-rw-r--r-- 1 root root   6774 Aug 15  2018 ksrsigner-20180815-221523.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6788 Aug 15  2018 ksrsigner-20180815-221858.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6798 Aug 15  2018 ksrsigner-20180815-222046.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6453 Aug 15  2018 ksrsigner-20180815-222210.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-3-C_to_C\033[0m
-rw-r--r-- 1 root root  14348 Aug 15  2018 ttyaudit-ttyS0-20180815-220248.log
-rw-r--r-- 1 root root  24749 Aug 15  2018 script-20180815.log
-rw-r--r-- 1 root root   6420 Feb 27  2019 ksrsigner-20190227-222718.log
drwxr-xr-x 2 root root   8192 Feb 27  2019 \033[01;34mKSK36\033[0m
-rw-r--r-- 1 root root  12372 Feb 27  2019 ttyaudit-ttyS0-20190227-221242.log
-rw-r--r-- 1 root root  22453 Feb 27  2019 script-20190227.log
-rw-r--r-- 1 root root   6252 Aug 14  2019 ksrsigner-20190814-215719.log
drwxr-xr-x 2 root root   8192 Aug 14  2019 \033[01;34mKSK38\033[0m
-rw-r--r-- 1 root root    357 Aug 14  2019 keybackup-20190814-231635.log
-rw-r--r-- 1 root root    210 Aug 14  2019 keybackup-20190814-231754.log
-rw-r--r-- 1 root root   1493 Aug 14  2019 KSKSlotDB.db
-rw-r--r-- 1 root root    271 Aug 14  2019 keybackup-20190814-231804.log
-rw-r--r-- 1 root root   6267 Aug 15  2019 ksrsigner-20190815-002322.log
-rw-r--r-- 1 root root  89867 Aug 15  2019 ttyaudit-ttyS0-20190814-213756.log
-rw-r--r-- 1 root root  29833 Aug 15  2019 script-20190814.log
-rw-r--r-- 1 root root      0 Feb 16 02:08 script-20200216.log
-rw-r--r-- 1 root root  11370 Feb 16 02:25 ttyaudit-ttyS0-20200216-020929.log
drwxr-xr-x 2 root root   8192 Feb 16 02:25 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root   6280 Feb 16 02:25 ksrsigner-20200216-022133.log
drwxr-xr-x 2 root root   8192 Feb 16 02:25 \033[01;34mKSK40\033[0m

./KSK30-0-D_to_E:
total 120
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214009
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr-root-2017-q4-0-d_to_e.xml

./KSK30-1-E_to_D:
total 120
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214402
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr-root-2017-q4-1-e_to_d.xml

./KSK30-2-D_to_D:
total 120
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214602
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr-root-2017-q4-2-d_to_d.xml

./KSK30-3-C_to_C:
total 104
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214756
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 20347 Aug 17  2017 skr-root-2017-q4-3-c_to_c.xml

./KSK32-0-D_to_E:
total 128
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207224219
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr-root-2018-q2-0-d_to_e.xml

./KSK32-1-E_to_D:
total 128
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207224724
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr-root-2018-q2-1-e_to_d.xml

./KSK32-2-D_to_D:
total 128
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207224920
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr-root-2018-q2-2-d_to_d.xml

./KSK32-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207225053
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 20347 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 20347 Feb  7  2018 skr-root-2018-q2-3-c_to_c.xml

./KSK34-0-D_to_E:
total 128
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815221523
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr-root-2018-q4-0-d_to_e.xml

./KSK34-1-E_to_D:
total 128
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815221858
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr-root-2018-q4-1-e_to_d.xml

./KSK34-2-D_to_D:
total 128
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815222046
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr-root-2018-q4-2-d_to_d.xml

./KSK34-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815222210
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 20349 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 20349 Aug 15  2018 skr-root-2018-q4-3-c_to_c.xml

./KSK36:
total 112
```

```
-rw-r--r-- 1 root root 29640 Feb 20  2019 skr.xml.20190227222718
-rw-r--r-- 1 root root 19600 Feb 20  2019 ksr-root-2019-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb 20  2019 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 27  2019 skr.xml
-rw-r--r-- 1 root root 20369 Feb 27  2019 skr-root-2019-q2-0.xml

./KSK38:
total 104
-rw-r--r-- 1 root root 20369 Aug  6  2019 skr.xml.20190814215719
-rw-r--r-- 1 root root 19600 Aug  6  2019 ksr-root-2019-q4-0.xml
-rw-r--r-- 1 root root  1148 Aug  6  2019 kskschedule.json
-rw-r--r-- 1 root root 20369 Aug 14  2019 skr.xml
-rw-r--r-- 1 root root 20369 Aug 14  2019 skr-root-2019-q4-0.xml

./tmp:
total 72
-rw-r--r-- 1 root root 1768 Feb 16 02:25 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.3
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Feb 16 02:25 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Feb 16 02:25 skr.keybundle.0

./KSK40:
total 104
-rw-r--r-- 1 root root 20369 Feb  4 23:14 skr.xml.20200216022133
-rw-r--r-- 1 root root 19600 Feb  4 23:14 ksr-root-2020-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb  4 23:14 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16 02:25 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16 02:25 skr-root-2020-q2-0.xml
root@coen:/media/HSMFD# umount /media/KSR/
root@coen:/media/HSMFD#HSMFD# exit
exit

Script done on Sun Feb 16 02:38:38 2020
```

```
2020-02-16T02:10:26+0000 ttyS0 ü
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0 BBL CRC32: 0x757574CA
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0 Running applicationBootLoader at 0xEFDC0000
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:26+0000 ttyS0 ABL CRC32: 0xE7E0FA6A
2020-02-16T02:10:26+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 ####################################
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 ###     ABL tamper records       ###
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 ####################################
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 ==================================
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 vextoosTamperCount:     0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 vintoosTamperCount:     14
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 vbboosTamperCount:      0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 maxstrtempTamperCount:  0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 minstrtempTamperCount:  0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 meshTamperCount:        0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 extampSMKTamperCount:   0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 extampIMKTamperCount:   0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 tempdiffTamperCount:    0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 pfTamperCount:          14
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 restartTamperCount:     45
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 Current tamper bitmaps:
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 ======================
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
```

```
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0   Bitmapped Change Record (most recent first):
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0   ========================================
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:27+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Running cryptoApplication at 0xEBF00000
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Jumping to startup @ 0x001037B4
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Board is P2020RDB
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   board_smp_init: 2 cpu
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Starting next program at v0015183c
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Starting K-Series Kernel
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:28+0000 ttyS0   Copyright AEP Networks Ltd. All Rights Reserved.
2020-02-16T02:10:28+0000 ttyS0
2020-02-16T02:10:29+0000 ttyS0   Sun Feb 16 00:41:02 2020
2020-02-16T02:10:29+0000 ttyS0
2020-02-16T02:10:29+0000 ttyS0   Starting auditd v2.0 ... started.
2020-02-16T02:10:29+0000 ttyS0
2020-02-16T02:10:29+0000 ttyS0   Interface 0 configured for IPv6.
2020-02-16T02:10:29+0000 ttyS0
2020-02-16T02:10:30+0000 ttyS0   Interface 0 configured for IPv4.
2020-02-16T02:10:30+0000 ttyS0
2020-02-16T02:10:30+0000 ttyS0   route: writing to routing socket: Network is unreachable
2020-02-16T02:10:30+0000 ttyS0
2020-02-16T02:10:30+0000 ttyS0   add net default: gateway ::: Network is unreachable
2020-02-16T02:10:30+0000 ttyS0
2020-02-16T02:10:30+0000 ttyS0   route: writing to routing socket: Network is unreachable
2020-02-16T02:10:30+0000 ttyS0
2020-02-16T02:10:30+0000 ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2020-02-16T02:10:30+0000 ttyS0
2020-02-16T02:10:30+0000 ttyS0   Starting USB driver...
2020-02-16T02:10:30+0000 ttyS0
2020-02-16T02:10:31+0000 ttyS0   9860 v2.3 Keyper Application - Nov  8 2013 13:17:33
2020-02-16T02:10:31+0000 ttyS0
2020-02-16T02:10:31+0000 ttyS0
2020-02-16T02:10:31+0000 ttyS0
2020-02-16T02:10:36+0000 ttyS0
2020-02-16T02:10:36+0000 ttyS0
2020-02-16T02:10:36+0000 ttyS0   Running DES POST Test
2020-02-16T02:10:36+0000 ttyS0
```

```
2020-02-16T02:10:36+0000        ttyS0   DES POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running Triple DES POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Triple DES POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running AES POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   AES POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running SHA1 POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   SHA1 POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running SHA2 POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   SHA2 POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running RandomGen POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   RandomGen POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running RSA POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   RSA POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running DSA POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   DSA POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   Running ECC POST Test
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:36+0000        ttyS0   ECC POST Test Passed
2020-02-16T02:10:36+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0   Audit on 16/2/2020 00:41:09 00100008
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0   Keyper 9860-2  Serial Number H1411006
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:37+0000        ttyS0   Memory Usage:
2020-02-16T02:10:37+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   RAM (free/total)        197Mb/256Mb
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   Flash (free/total)      127Mb/128Mb
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0      black store          440b
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0      statistics           112b
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0      other                116b
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   RedStore (free/total)   109Kb/128Kb
```

```
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   Network Configuration:
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   IPv4: enabled
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   IPv6: enabled
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   MAC/IP address(es): 00:E0:06:C0:B3:1B / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b31b/64
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   HSM Port: 05000
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   HSM Gateway(s): 0.0.0.0 ::
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   Software Versions:
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   BBL 010 ABL 011 App 023
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   CPLD Version:
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   1.9
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   SCR Firmware Version:
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   OROS-R2.99-R1.20
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   HmcListener: Created IPv4 socket 10 on port 3000.
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   HmcListener: Created IPv6 socket 11 on port 3000.
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:10:38+0000        ttyS0   Audit on 16/2/2020 00:41:11 00100003
2020-02-16T02:10:38+0000        ttyS0
2020-02-16T02:17:17+0000        ttyS0   Audit on 16/2/2020 00:47:49 00200069 0A400000B706296E
2020-02-16T02:17:17+0000        ttyS0
2020-02-16T02:17:28+0000        ttyS0   Audit on 16/2/2020 00:48:01 0020006a
2020-02-16T02:17:28+0000        ttyS0
2020-02-16T02:18:04+0000        ttyS0   Audit on 16/2/2020 00:48:37 00200069 0A400000B646296E
2020-02-16T02:18:04+0000        ttyS0
2020-02-16T02:18:16+0000        ttyS0   Audit on 16/2/2020 00:48:48 0020006a
2020-02-16T02:18:16+0000        ttyS0
2020-02-16T02:18:39+0000        ttyS0   Audit on 16/2/2020 00:49:12 00200069 0A400000B7C6296E
2020-02-16T02:18:39+0000        ttyS0
2020-02-16T02:18:43+0000        ttyS0
2020-02-16T02:18:43+0000        ttyS0
```

```
2020-02-16T02:18:43+0000        ttyS0   TcpListener: Created IPv4 socket 15 on port 5000.
2020-02-16T02:18:43+0000        ttyS0
2020-02-16T02:18:43+0000        ttyS0
2020-02-16T02:18:43+0000        ttyS0
2020-02-16T02:18:43+0000        ttyS0   TcpListener: Created IPv6 socket 16 on port 5000.
2020-02-16T02:18:43+0000        ttyS0
2020-02-16T02:18:43+0000        ttyS0   Audit on 16/2/2020 00:49:16 00100002
2020-02-16T02:18:43+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0   TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0   CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:21:56+0000        ttyS0   TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2020-02-16T02:21:56+0000        ttyS0
2020-02-16T02:25:48+0000        ttyS0
2020-02-16T02:25:48+0000        ttyS0
2020-02-16T02:25:48+0000        ttyS0   CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2020-02-16T02:25:48+0000        ttyS0
2020-02-16T02:33:22+0000        ttyS0   Audit on 16/2/2020 01:03:55 00200069 0A400000B706296E
2020-02-16T02:33:22+0000        ttyS0
2020-02-16T02:33:44+0000        ttyS0   Audit on 16/2/2020 01:04:16 00200069 0A400000B646296E
2020-02-16T02:33:44+0000        ttyS0
2020-02-16T02:34:04+0000        ttyS0   Audit on 16/2/2020 01:04:37 00200069 0A400000B7C6296E
2020-02-16T02:34:04+0000        ttyS0
2020-02-16T02:34:06+0000        ttyS0
2020-02-16T02:34:06+0000        ttyS0
2020-02-16T02:34:06+0000        ttyS0   TcpListener: Closed IPv4 socket 15 on port 5000.
2020-02-16T02:34:06+0000        ttyS0
2020-02-16T02:34:06+0000        ttyS0
2020-02-16T02:34:06+0000        ttyS0
2020-02-16T02:34:06+0000        ttyS0   TcpListener: Closed IPv6 socket 16 on port 5000.
2020-02-16T02:34:06+0000        ttyS0
2020-02-16T02:34:09+0000        ttyS0   Audit on 16/2/2020 01:04:39 00100003
2020-02-16T02:34:09+0000        ttyS0
```

Place HSM Cards into TEBs

Step	Activity	Initials	Time
23	The CA calls each of the COs listed below sequentially 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 their 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 aloud the TEB number and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony 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 card to the CO. h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. i) Repeat steps for the 2 SO cards respectively, ensuring they're facing outward in the plastic case and placed into the prepared SO TEB. j) CO writes the date and time, then signs the table of IW's script, then IW initials the entry. k) CO returns to their seat with their credentials, being especially careful not to compromise any TEB. l) Repeat steps for all the remaining COs on the list. **CO1: Arbogast Fabian** **OP TEB # BB91951351** **SO TEB # ~~BB91951352~~** BB46584377 **CO3: João Damas** **OP TEB # BB91951353** **SO TEB # ~~BB91951354~~** BB46584455 **CO7: Subramanian Moonesamy** **OP TEB # BB91951355** **SO TEB # ~~BB91951356~~** BB46584385	YG.	03:07

TCR	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	OP 1 of 7 SO 1 of 7	OP TEB # BB91951351 SO TEB # ~~BB91951352~~ BB46584377	Arbogast Fabian		2020 Feb 16	03:02	YG.
CO3	OP 3 of 7 SO 3 of 7	OP TEB # BB91951353 SO TEB # ~~BB91951354~~ BB46584455	João Damas		2020 Feb 16	03:05	YG.
CO7	OP 7 of 7 SO 7 of 7	OP TEB # BB91951355 SO TEB # ~~BB91951356~~ BB46584385	Subramanian Moonesamy		2020 Feb 16	03:06	YG.

Return the Equipment to Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
24	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)	YG.	03:09
25	SSC1 opens Safe #1 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.**	YG.	03:10
26	SSC1 removes the safe log, then writes the date and time, then signs 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.**	YG.	03:11
27	CA performs the following steps to return each piece of equipment to the safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where **"Return"** is indicated. d) IW verifies the safe log entry, then initials it. **HSM4: TEB # BB51184238** **Laptop4: TEB # BB81420119** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951350**	YG.	03:13

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
28	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.	YG.	03:14
29	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	Y.G.	03:14
30	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	YG	03:16

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
31	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)	YG	03:17
32	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping on the first number in the combination.**	YG.	03:18
33	SSC2 removes the safe log, then writes the date and time, then signs 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.**	YG	03:19

COs Return the Credentials to Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
34	COs perform the following steps sequentially to return the required TEBs: a) CO reads aloud the TEB number(s), then verifies integrity while showing the TEB(s) to the audit camera above b) After the CA operates the guard key in the bottom lock, CO uses their tenant key to operate the top lock and open their safe deposit box. c) CO reads aloud the safe deposit box number, places their TEB(s) inside, then locks the safe deposit box. **Note: The COs will retrieve their new safe deposit box keys when specified below.** d) CO writes the date and time, then signs the safe log where **"Return"** is indicated. e) IW verifies the completed safe log entry, then initials it. **CO1: Arbogast Fabian** **Box # 1788 (Retrieve keys from lock)** **OP TEB # BB91951351** **SO TEB # ~~BB91951352~~** BB46584377 **CO3: João Damas** **Box # 1069 (Retrieve keys from lock)** **OP TEB # BB91951353** **SO TEB # ~~BB91951354~~** BB46584455 **CO7: Subramanian Moonesamy** **Box # 1790 (Retrieve keys from lock)** **OP TEB # BB91951355** **SO TEB # ~~BB91951356~~** BB46584385	YG.	03:26

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
35	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry, then initials it.	YG.	03:27
36	SSC2 returns the safe log back to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	YG.	03:27
37	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	YG	03:28

Act 6: Close the Key Signing Ceremony

The CA will finish the ceremony by:

- Reading any exceptions that occurred during the ceremony
- Calling the ceremony participants to sign the IW's script
- Stopping the online streaming and video recording
- Ensuring that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Preparing the audit bundle materials

Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.	YG	03:30
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.**	YG	03:32
3	CA reviews IW's script, then signs the participants list.	YG	03:36
4	IW signs the list and records the completion time.	YG	03:36

Stop Online Streaming and Post Ceremony Information

Step	Activity	Initials	Time
5	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.	YG	03:37
6	CA informs onsite participants of post ceremony activities.	YG	03:37
7	Ceremony participants take a group photo.	YG	03:39

Sign Out of Tier 4 (Key Ceremony Room) and Stop Recording

Step	Activity	Initials	Time
8	RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.) SA, IW, and CA must remain in Tier 4 (Key Ceremony Room.)	YG	03:44
9	CA requests that an SA stop the audit camera video recording.	YG	03:44

Bundle Audit Materials

Step	Activity	Initials	Time
10	IW makes a copy of their script for off-site audit bundle containing: 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: **20190814 00:00:00 to 20200216 00:00:00 UTC** e) IW's attestation (Appendix C). f) SA's attestation (Appendix D and E). All TEBs are labeled **Root DNSSEC KSK Ceremony 40**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	YG	04:20

Appendix A: References

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

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

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

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

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

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

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

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

The following is the main command invoked by this script:
`find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist`[2]
Note: The sort command has a different behavior depending on the locale settings specified in environment variables. Current OS locale setting is `LC_COLLATE="POSIX"`

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

[5] **`ttyaudit:`** Is a perl script use to capture and logging the *HSM* output.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

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

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

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

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

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

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

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

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

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

Two electronic copies of the following:

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

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

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

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

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

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

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

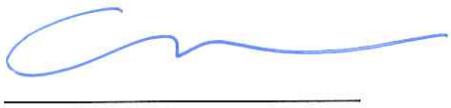
7. Other items

If applicable.

Appendix C: Key Ceremony Script (by IW)

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

IW: **Yuko Green**

Signature: 

Date: 2020 Feb 16

Appendix D: Access Control System Configuration Review (by SA)

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

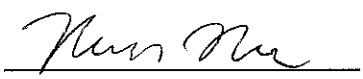
a) There were NO discrepancies found on the system configurations, assigned authorizations and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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

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

Range: **20190814 00:00:00 to 20200216 00:00:00 UTC.**

SA: Brian Martin

Signature: 

Date: 2020 Feb 16

Appendix E: Firewall Configuration Review (by SA)

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

SA: Brian Martin

Signature:

Date: 2020 Feb 16

```
## Last commit: 2020-01-17 18:22:39 UTC by jjenkins
version 15.1X49-D170.4;
system {
    host-name srx;
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    root-authentication {
        encrypted-password "XXX"; ## SECRET-DATA
    }
    name-server {
        192.0.42.53;
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        user sfreeark {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "XXX"; ## SECRET-DATA
            }
        }
        password {
            format sha512;
        }
    }
    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;
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
chassis {
    config-button no-rescue no-clear;
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
security {
    pki {
        ca-profile root-ca {
            ca-identity "ICANN Root CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
            administrator {
                email-address "cbo-team@iana.org";
            }
        }
        ca-profile intermediate-ca {
            ca-identity "ICANN SSL CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
        }
    }
    ike {
        proposal ike-proposal-KMF {
            authentication-method rsa-signatures;
            dh-group group24;
            authentication-algorithm sha-256;
            encryption-algorithm aes-256-cbc;
        }
        policy ike-policy-KMF {
            proposals ike-proposal-KMF;
            certificate {
                local-certificate ksk-lax;
            }
        }
        gateway Gateway-to-KMF-East {
            ike-policy ike-policy-KMF;
            address 64.124.6.5;
            local-identity distinguished-name;
            remote-identity distinguished-name;
            external-interface ge-0/0/15;
            version v2-only;
        }
    }
    ipsec {
        proposal IPSecProposal {
            protocol esp;
            authentication-algorithm hmac-sha-256-128;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 7200;
        }
        policy defaultPolicy {
            perfect-forward-secrecy {
                keys group5;
```

```
        }
        proposals IPSecProposal;
    }
    vpn vpn-to-KMF-East {
        bind-interface st0.1;
        ike {
            gateway Gateway-to-KMF-East;
            ipsec-policy defaultPolicy;
        }
        establish-tunnels immediately;
    }
}
screen {
    ids-option external-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
    }
}
nat {
    source {
        rule-set internal-to-external {
            from zone [ access guest wifi ];
            to zone untrust;
            rule source-nat-rule {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
policies {
    from-zone access to-zone untrust {
        policy allow-mail {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address [ icann-dns google-dns ];
                application [ junos-dns-udp junos-dns-tcp ];
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-simplex {
            match {
                source-address IDP;
                destination-address simplex;
                application any;
            }
            then {
                permit;
                log {
```

```
                session-close;
            }
        }
    }
}
from-zone access to-zone video {
    policy access-to-video {
        match {
            source-address IMS;
            destination-address kmf_west_video;
            application junos-icmp-all;
        }
        then {
            permit;
        }
    }
}
from-zone access to-zone ipsec {
    policy allow-access-to-ipsec {
        match {
            source-address [ ACS ACC ];
            destination-address [ kmf_east_acs kmf_east_acc ];
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy allow-access-access {
        match {
            source-address kmf_west_access;
            destination-address kmf_east_access;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ipsec to-zone access {
    policy allow-ipsec-to-access {
        match {
            source-address [ kmf_east_acs kmf_east_acc ];
            destination-address [ ACS ACC ];
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy allow-access-access {
        match {
            source-address kmf_east_access;
            destination-address kmf_west_access;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone video to-zone ipsec {
```

```
    policy allow-video-to-ipsec {
        match {
            source-address VSS;
            destination-address kmf_east_vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_west_video;
            destination-address kmf_east_video;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone guest to-zone untrust {
    policy allow-guest-to-untrust {
        match {
            source-address kmf_west_guest;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone wifi to-zone untrust {
    policy allow-wifi-to-untrust {
        match {
            source-address kmf_west_wifi;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ipsec to-zone video {
    policy allow-ipsec-to-video {
        match {
            source-address kmf_east_vss;
            destination-address VSS;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_east_video;
            destination-address kmf_west_video;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone access to-zone access {
    policy allow-access {
        match {
            source-address any;
            destination-address any;
```

```
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone video to-zone untrust {
        policy allow-mail {
            match {
                source-address VSS;
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
    }
    default-policy {
        deny-all;
    }
}
zones {
    security-zone access {
        address-book {
            address ACS 10.4.28.203/32;
            address ACC 10.4.28.202/32;
            address IDP 10.4.28.201/32;
            address EVM 10.4.28.200/32;
            address IMS 10.4.28.204/32;
            address E1 10.4.28.210/32;
            address E3 10.4.28.212/32;
            address E4 10.4.28.213/32;
            address kmf_west_access 10.4.28.192/26;
            address localnet 10.4.28.0/24;
            address-set iris-scanners {
                address E1;
                address E3;
                address E4;
            }
        }
        interfaces {
            irb.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        ntp;
                        ssh;
                    }
                }
            }
        }
    }
    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-0/0/15.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
            }
        }
```

```
        }
        security-zone video {
            address-book {
                address kmf_west_video 10.4.28.128/26;
                address VSS 10.4.28.150/32;
                address C1 10.4.28.151/32;
                address C2 10.4.28.152/32;
                address C3 10.4.28.153/32;
                address-set cameras {
                    address C1;
                    address C2;
                    address C3;
                }
            }
            interfaces {
                irb.1 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
        security-zone guest {
            address-book {
                address STR 10.4.28.20/32;
                address VCC 10.4.28.22/32;
                address kmf_west_guest 10.4.28.0/25;
            }
            interfaces {
                irb.2 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
        security-zone ipsec {
            address-book {
                address kmf_east_access 10.4.29.192/26;
                address kmf_east_video 10.4.29.128/26;
                address kmf_east_acs 10.4.29.204/32;
                address kmf_east_acc 10.4.29.202/32;
                address kmf_east_idp 10.4.29.201/32;
                address kmf_east_evm 10.4.29.200/32;
                address kmf_east_ims 10.4.29.203/32;
                address kmf_east_E1 10.4.29.210/32;
                address kmf_east_E2 10.4.29.211/32;
                address kmf_east_E3 10.4.29.212/32;
                address kmf_east_E4 10.4.29.213/32;
                address kmf_east_vss 10.4.29.150/32;
                address kmf_east_C1 10.4.29.151/32;
                address kmf_east_C2 10.4.29.152/32;
                address kmf_east_C3 10.4.29.153/32;
            }
            interfaces {
                st0.1 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                            ike;
                        }
                    }
                }
            }
        }
        security-zone wifi {
            address-book {
                address kmf_west_wifi 10.100.1.0/24;
            }
            interfaces {
                irb.3 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                        }
                    }
                }
            }
        }
    }
}
interfaces {
    ge-0/0/6 {
        ether-options {
```

```
            802.3ad ae0;
        ]
    }
    ge-0/0/7 {
        ether-options {
            802.3ad ae0;
        }
    }
    ge-0/0/15 {
        unit 0 {
            family inet {
                address 192.0.35.202/26;
            }
        }
    }
    ae0 {
        aggregated-ether-options {
            lacp {
                active;
            }
        }
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [ vlan-access vlan-guest vlan-video vlan-wifi ];
                }
            }
        ]
    }
    irb {
        unit 0 {
            description "access vlan";
            family inet {
                address 10.4.28.193/26;
            }
        }
        unit 1 {
            description "video vlan";
            family inet {
                address 10.4.28.129/26;
            }
        }
        unit 2 {
            description "guest vlan";
            family inet {
                address 10.4.28.1/25;
            }
        }
        unit 3 {
            description "wifi vlan";
            family inet {
                address 10.100.1.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input route-engine-filter;
                }
            }
        }
    }
    st0 {
        unit 1 {
            description "IPSec KMF-West";
            family inet;
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.0.35.201;
        route 10.4.29.0/24 next-hop st0.1;
        route 64.124.6.5/32 next-hop 192.0.35.201;
    }
}
policy-options {
    prefix-list resolver-servers {
        apply-path "system name-server <*>";
    }
    prefix-list local-prefixes {
        10.4.28.0/24;
    }
    prefix-list ntp-servers {
        129.6.15.28/32;
```

```
        129.6.15.29/32;
    }
    prefix-list remote-ike-peers {
        apply-path "security ike gateway <*> address <*>";
    }
}
firewall {
    family inet {
        filter route-engine-filter {
            term deny-icmp-redirects {
                from {
                    protocol icmp;
                    icmp-type redirect;
                }
                then {
                    discard;
                }
            }
            term allow-icmp {
                from {
                    protocol icmp;
                    icmp-type [ echo-request echo-reply unreachable time-exceeded ];
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-traceroute {
                from {
                    protocol udp;
                    port 33434-33534;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-dns {
                from {
                    source-prefix-list {
                        resolver-servers;
                    }
                    protocol udp;
                    source-port domain;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-ntp {
                from {
                    source-prefix-list {
                        local-prefixes;
                        ntp-servers;
                    }
                    protocol udp;
                    port ntp;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-establish {
                from {
                    protocol tcp;
                    tcp-established;
                }
                then accept;
            }
            term allow-ipsec-esp {
                from {
                    source-prefix-list {
                        remote-ike-peers;
                    }
                    protocol esp;
                }
                then accept;
            }
            term allow-ipsec-udp {
                from {
                    source-prefix-list {
                        remote-ike-peers;
                    }
                    protocol udp;
                    port 500;
```

```
                }
                then accept;
            }
            term allow-ike-fragments {
                from {
                    source-prefix-list {
                        remote-ike-peers;
                    }
                    is-fragment;
                    protocol udp;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-ssh {
                from {
                    source-address {
                        10.4.29.193/32;
                    }
                    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;
    }
}
vlans {
    vlan-access {
        vlan-id 10;
        l3-interface irb.0;
    }
    vlan-guest {
        vlan-id 12;
        l3-interface irb.2;
    }
    vlan-video {
        vlan-id 11;
        l3-interface irb.1;
    }
    vlan-wifi {
        vlan-id 13;
        l3-interface irb.3;
    }
}
bmartin@srx>
```