Root DNSSEC KSK Ceremony 41

Thursday April 23, 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 5th Edition (2020-04-07)

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

Participants

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

Title / Roles	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		2020 Apr 23	20:16
IW	Jonathan Denison / ICANN			
SSC1	Sabrina Tanamal / PTI			
SSC2	Anand Mishra / ICANN			
SA	Patrick Tudor / ICANN	TUD 012		
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			

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 a 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 a CA, IW, or SA 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
- During a ceremony a CA, IW, or SA may escort participants out of Tier 4 (Key Ceremony Room) at the CA's discretion if Tier 5 (Safe Room) is not occupied
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log located in Tier 3
- The SA starts filming before the majority of participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step in order to attest to the ceremony's proper performance
- The CA reads each step aloud prior to its performance
- Upon the successful completion of a step, the IW will announce and record its time of completion, and initials that step in their script
- A ceremony participant who has cause for concern or detects an issue is encouraged to interrupt the ceremony for discussion. The issue is brought to resolution before the ceremony resumes
- 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 recite and/or confirm identifiers comprised of numbers and letters. When spelling identifiers, the phonetic alphabet shown below should 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 into Tier 5 (Safe Room) to retrieve the following materials:

- Safe #1: HSM, laptop, OS DVD, etc
- Safe #2: The COs' 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.	JD	17:06
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.	JD	17:06
3	CA asks that any first time ceremony participants in the room introduce themselves.	JD	17:06
4	CA confirms that additional required personnel including COs, RZM, and Auditors are connected to the remote call. Scheduled remote participants are: **CO4: Carlos Martinez** (Key scripted for use) 17:07 **CO5: Olafur Gudmundsson** (Key scripted for use) 17:07 **CO6: Nicolas Antoniello** (Key scripted for use) 17:07 **CO3: Joao Damas** (Key designated as backup) 17:07 **RZM: Duane Wessels / Verisign** 17:07 **RZM: Trevor Davis / Verisign** 17:07 **AUD: James Kim / RSM** 17:07	JD	17:08

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
5	CA reviews emergency evacuation procedures with onsite participants.	JD	17:08
6	CA explains the use of personal electronic devices during the ceremony.	JD	17:08
7	CA summarizes the purpose of the ceremony.	JD	17:10

Verify the Time and Date

Step	Activity	Initials	Time
8	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: 2020/04/23 17:11 **Note: All entries into this script or any logs should follow this common source of time.**	JD	17:11

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Carlos Martinez, am hereby entrusting my safe deposit box key enclosed in TEB # BB919S1284 for safe deposit box #1068 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name CARLOS MARTINEZ

Signature Carlos Martinez

Date April 13, 2020

* TEB # : BB 919 51 284

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Olafur Gudmundsson, am hereby entrusting my safe deposit box key enclosed in TEB # BB 9195127 for safe deposit box #1789 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name ÓLAFUR GUÐMUNDSSON

Signature Ólafur Guð

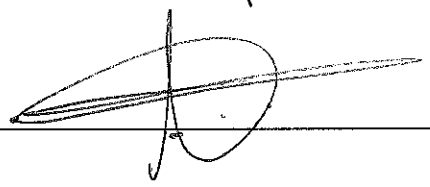
Date 2020/4/11

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Nicolas Antoniello, am hereby entrusting my safe deposit box key enclosed in TEB # BB91951289 for safe deposit box #1073 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name Nicolás Antoniello

Signature 

Date 14/4/2020

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I, Joao Luis Silva Damas, am hereby entrusting my safe deposit box key enclosed in TEB # BB91951281 for safe deposit box #1069 located within Safe #2 at the key management facility in El Segundo, CA.

I understand that the safe deposit box key will be safeguarded within its enclosed TEB until the time it is required to perform disaster recovery operations in an audited ceremony environment. The TEB will be examined by the Ceremony Administrator before the key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the tenant key, and provide authorization remotely, if possible, when the key ceremony script requires use of the safe deposit box key. I understand the chain of custody of my safe deposit box key will be protected and documented until it is returned.

Printed Name JOÃO LUIS SILVA DAMAS

Signature JLSD

Date 15/4/2020

Crypto Officer Key Verification

Step	Activity	Initials	Time
9	The CA performs the following steps to verify the listed CO keys: a) Remove the TEB from the shipping envelope and discard the shipping envelope. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and place it on the ceremony table visible to the audit camera. d) Open the TEB and place its contents on the ceremony table. e) Give the CO key declaration to IW to verify the TEB number, and then insert in the audit bundle. f) Discard the TEB. g) Attach the CO tenant key to its corresponding pre-labeled key ring. h) Give the CO tenant key to the IW. **CO4: Carlos Martinez** **Key TEB # BB91951284** (See Appendix F on page 35) **CO5: Olafur Gudmundsson** **Key TEB # BB91951277** (See Appendix G on page 36) **CO6: Nicolas Antoniello** **Key TEB # BB91951289** (See Appendix H on page 37) **Note 1: The CO3 Joao Damas Safe Deposit Box Key TEB # BB91951281 has been designated as a backup. See Appendix I on page 38.** **Note 2: The COs' tenant keys were individually transmitted to separate trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.**	JD	17:23

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
10	CA and IW transport a flashlight, and escort SSC2 into Tier 5 (Safe Room.)	JD	17:24
11	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.**	JD	17:26
12	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.	JD	17:28

Extract CO Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
13	IW performs the following steps sequentially to retrieve the required TEBs: a) IW announces the name of the CO whose credentials will be extracted and CO confirms their authorization to open their safe deposit box. b) When the CO provides confirmation, the CA operates the guard key in the bottom lock, then the IW uses the CO's tenant key to operate the top lock and open their safe deposit box. c) IW reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB. d) IW reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above. e) IW retains the TEB(s) specified below, returns any TEBs not required, then closes and locks the safe deposit box with assistance from the CA. f) IW writes the date and time, then signs the safe log where **"Remove"** is indicated. g) CA verifies the completed safe log entries, then initials it. **CO4: Carlos Martinez** **Box # 1068** **OP TEB # BB46592092 (Retain)** **SO TEB # BB46584665 (Check and Return)** **CO5: Olafur Gudmundsson** **Box # 1789** **OP TEB # BB46584380 (Retain)** **SO TEB # BB46584381 (Check and Return)** **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB46584382 (Retain)** **SO TEB # BB46584383 (Check and Return)**	JD	17:46

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
14	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.	JD	17:46
15	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.	JD	17:47
16	CA, IW, and SSC2 leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	JD	17:48
17	IW places the TEBs on the ceremony table.	JD	17:48

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
18	CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)	JD	17:49
19	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.**	JD	17:51
20	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.	JD	17:52

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

Step	Activity	Initials	Time
21	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 (Check and Return)** ***Last Verified: KSK40-AC 2020-02-16*** **HSM4: TEB # BB51184238 (Check and Return)** ***Last Verified: KSK40 2020-02-16*** **HSM5W: TEB # BB51184237 (Place on Cart)** ***Last Verified: KSK40-AC 2020-02-16*** **Laptop3: TEB # BB81420125 (Place on Cart)** ***Last Verified: KSK38 2019-08-14*** **Laptop4: TEB # BB81420119 (Check and Return)** ***Last Verified: KSK40 2020-02-16*** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951350 (Place on Cart)** ***Last Verified: KSK40 2020-02-16*** **KSK-2017: TEB # BB46584387 (Check and Return)** ***Last Verified: KSK38 2019-08-14*** **Note: *"Last verified"* indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**	JD	18:01

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

Step	Activity	Initials	Time
22	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.	JD	18:02
23	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.	JD	18:02
24	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	JD	18:03

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. **HSM5W: TEB # BB51184237 / Serial # H1903017** ***Last Verified: KSK40-AC 2020-02-16*** **Laptop3: TEB # BB81420125 / Service Tag # C8SVSG2** ***Last Verified: KSK38 2019-08-14*** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951350** ***Last Verified: KSK40 2020-02-16*** **Note: *"Last verified"* indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**	JD	18:10
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.	JD	18:11
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** after the laptop power is switched ON.	JD	18:14
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**	JD	18:15

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 < /dev/sr0` b) 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/41**	JD	18:13

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`	JD	18:19

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 "20200423 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.	JP	18:20

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the **Ceremony 40 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.	JD	18:21
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash -c` CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script. 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 vagabond facial perceptive suspense hideaway southward tambourine Scotland insincere backward savagery ahead visitor upset Istanbul cowbell decadence frighten headwaters uproot examine snowcap intention IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 40 annotated script.	JD	18:24

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 40** and the sheet of paper with the printed HSMFD hash to RKOS.	JD	18:25

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`	JD	18:25
12	CA executes the command below to log activities of the **Commands** terminal window: `script script-20200423.log`	JD	18:25

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 /dev/ttyS0`
	Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.
		JD	18:27

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM5W** b) Ensure an RJ45 blockout is present in the **"MGMT"** port of the HSM. Install one if not present. c) Plug the null modem cable into the serial port of the HSM. d) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H1903017**, then scroll back to the bottom. **HSM5W: Serial # H1903017** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	JD	18:36

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 COs' 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 containing 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

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
1	CA performs the following steps to verify the COs' credentials: a) Read aloud the TEB number, then inspect it for tamper evidence. b) Open the TEB, then remove the plastic case containing the card(s). c) Open the plastic case, then place the enclosed card(s) on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table. **CO4: Carlos Martinez** **OP TEB # BB46592092** **CO5: Olafur Gudmundsson** **OP TEB # BB46584380** **CO6: Nicolas Antoniello** **OP TEB # BB46584382**	JD	18:34

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 4 of 7 2nd OP card 5 of 7 3rd OP card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	JD	18:36

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.	JD	18:39

4	CA performs the following steps to test the network connectivity between laptop and HSM:
	a) Use the **Commands** terminal window
	b) Test connectivity by executing:
	`ping hsm`
	c) Wait for responses, then exit by pressing:
	`Ctrl + C`
		JD	18:39

Insert the KSRFD

Step	Activity	Initials	Time
5	CA plugs the FD labeled **"KSR"** into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window. **Note: The KSRFD was transferred to the facility by the RKOS. It contains 3 KSRs. One for the next calendar quarter and the remaining for subsequent quarter(s).**	JD	18:41

Execute the KSR Signer for KSR 2020 Q3

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK41-2020-Q3/ksr-root-2020-q3-0.xml`	JD	18:42
7	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	JD	18:42

VERISIGN™

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

Verisign.com

April 22nd, 2020

To Whom It May Concern:

This is a letter of Verification of Employment for Trevor Lewis Davis. VeriSign, Inc. ("Verisign") has employed Trevor Lewis Davis full-time since September 29th, 2014, currently as Manager - CBO in our Production Operations organization.

Verisign, a global provider of domain name registry services and internet infrastructure, enables internet navigation for many of the world's most recognized domain names. Verisign enables the security, stability, and resiliency of key internet infrastructure and services, including providing root zone maintainer services, operating two of the 13 global internet root servers, and providing registration services and authoritative resolution for the .com and .net top-level domains, which support the majority of global e-commerce. To learn more about what it means to be Powered by Verisign, please visit Verisign.com.

For more than 22 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 158.8 million .com and .net domain names and processing more than 210 billion query transactions daily-keeping the world connected online, seamlessly and securely. Verisign is experienced in and provides support for both IPv6 and DNSSEC.

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

Sincerely,

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

VERISIGN™

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

23 April 2020

The SHA256 hash of the 2020 Q3 KSR file is:

ksr-root-2020-q3-0.xml:

7b5188b568b4e932d9ac26df804d28adbc09d70f186bafcc2ff067718bf9b973

The PGP wordlist for the hash above is:

PGP Words: kickoff enchanting newborn positive frighten politeness treadmill component sugar penetrate bookshelf therapist merit disruptive breadline perceptive showgirl applicant stopwatch atmosphere beaming Hamilton rocker revolver cement upcoming freedom hideaway obtuse Waterloo sentence hurricane

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.

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

23 April 2020

The SHA256 hash of the 2020 Q4 KSR file is:

ksr-root-2020-q4-0.xml:

e3068f0cfc5a69ce2c62e12295597607b099d3f1e6c99eb37b6fdbf77fc2f8a1

The PGP wordlist for the hash above is:

PGP Words: tissue amulet payday article wayside existence gazelle sardonic Burbank gadgetry tempest candidate preclude examine inverse amusement ruffled nebula stapler vacancy tracker retrospect quiver pocketful kickoff hemisphere suspense voyager lockup repellent Vulcan outfielder

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.

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

23 April 2020

The SHA256 hash of the 2021 Q1 KSR file is:

ksr-root-2021-q1-0.xml:

2dd682ff1bdbdc746c1324b663793eb813c1aedd593f96ff8f3cc819dfe30643

The PGP wordlist for the hash above is:

PGP Words: button speculate miser Yucatan beeswax suspicious sweatband hydraulic glucose barbecue bluebird potato flatfoot inertia concert provincial Aztec recover robust tambourine endow customer prefer Yucatan payday crossover spaniel bottomless talon torpedo afflict decimal

Attested on behalf of VeriSign by:

Trevor Davis
Manager
Cryptographic Business Operations
VeriSign, Inc.

Verify the KSR Hash for KSR 2020 Q3

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed in the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themself. The IW verifies employment documents and identification **off camera** for the purpose of authentication while maintaining privacy. **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 the KSR(s), 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 in advance to be included in the final annotated script and audit bundle.** TREVOR LEWIS DAVIS (REMOTE PARTICIPANT) c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.	JD	18:45
9	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"**	JD	18:47
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/KSK41-2020-Q3/skr-root-2020-q3-0.xml`	JD	18:47

Execute the KSR Signer for KSR 2020 Q4

Step	Activity	Initials	Time
11	CA executes the command below in the terminal window to copy the previous quarter generated SKR, in order to construct a chain of trust to the next KSR: `cp /media/KSR/KSK41-2020-Q3/skr-root-2020-q3-0.xml /media/KSR/KSK41-2020-Q4/skr.xml`	JD	18:49
12	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK41-2020-Q4/ksr-root-2020-q4-0.xml` **Note: It is expected that the KSR Signer Software will issue a `warning` since the requests signature will exceeds the limit of 180 days of expiration in the future. This additional SKR will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set would not expire more than 180 days in the future.**	JD	18:50
13	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	JD	18:51

Verify the KSR Hash for KSR 2020 Q4

Step	Activity	Initials	Time
14	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	JD	18:52
15	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"**	JD	18:52
16	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in: `/media/KSR/KSK41-2020-Q4/skr-root-2020-q4-0.xml`	JD	18:52

Execute the KSR Signer for KSR 2021 Q1

Step	Activity	Initials	Time
17	CA executes the command below in the terminal window to copy the previous quarter generated SKR, in order to construct a chain of trust to the next KSR: `cp /media/KSR/KSK41-2020-Q4/skr-root-2020-q4-0.xml /media/KSR/KSK41-2021-Q1/skr.xml`	JD	18:54
18	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK41-2021-Q1/ksr-root-2021-q1-0.xml` **Note: It is expected that the KSR Signer Software will issue a `warning` since the requests signature will exceeds the limit of 180 days of expiration in the future. This additional SKR will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set would not expire more than 180 days in the future.**	JD	18:54
19	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	JD	18:54

Verify the KSR Hash for KSR 2021 Q1

Step	Activity	Initials	Time
20	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	JD	18:55
21	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"**	JD	18:56
22	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in: `/media/KSR/KSK41-2021-Q1/skr-root-2021-q1-0.xml`	JD	18:56

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
23	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) `for i in $(ls -1 ksrsigner-202004*.log); do printlog $i; done`	JD	18:58
24	IW attaches a copy of the required ksrsigner log to their script.	JD	18:59

```
Starting: ksrsigner /media/KSR/KSK41-2020-Q3/ksr-root-2020-q3-0.xml (at Thu Apr 23 18:42:08 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:          H1903017

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

Validate and Process KSR /media/KSR/KSK41-2020-Q3/ksr-root-2020-q3-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-07-01T00:00:00 2020-07-22T00:00:00  46594,48903
2  2020-07-11T00:00:00 2020-08-01T00:00:00  46594
3  2020-07-21T00:00:00 2020-08-11T00:00:00  46594
4  2020-07-31T00:00:00 2020-08-21T00:00:00  46594
5  2020-08-10T00:00:00 2020-08-31T00:00:00  46594
6  2020-08-20T00:00:00 2020-09-10T00:00:00  46594
7  2020-08-30T00:00:00 2020-09-20T00:00:00  46594
8  2020-09-09T00:00:00 2020-09-30T00:00:00  46594
9  2020-09-19T00:00:00 2020-10-10T00:00:00  26116,46594
...PASSED.

SHA256 hash of KSR:
7B5188B568B4E932D9AC26DF804D28ADBC09D70F186BAFCC2FF067718BF9B973
>> kickoff enchanting newborn positive frighten politeness treadmill component sugar penetrate bookshelf therapist merit
disruptive breadline perceptive showgirl applicant stopwatch atmosphere beaming Hamilton rocker revolver cement upcoming
freedom hideaway obtuse Waterloo sentence hurricane <<

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/KSK41-2020-Q3/skr-root-2020-q3-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-07-01T00:00:00 2020-07-22T00:00:00  46594,48903   20326(Klajeyz)/S
2  2020-07-11T00:00:00 2020-08-01T00:00:00  46594         20326(Klajeyz)/S
3  2020-07-21T00:00:00 2020-08-11T00:00:00  46594         20326(Klajeyz)/S
4  2020-07-31T00:00:00 2020-08-21T00:00:00  46594         20326(Klajeyz)/S
5  2020-08-10T00:00:00 2020-08-31T00:00:00  46594         20326(Klajeyz)/S
6  2020-08-20T00:00:00 2020-09-10T00:00:00  46594         20326(Klajeyz)/S
7  2020-08-30T00:00:00 2020-09-20T00:00:00  46594         20326(Klajeyz)/S
8  2020-09-09T00:00:00 2020-09-30T00:00:00  46594         20326(Klajeyz)/S
9  2020-09-19T00:00:00 2020-10-10T00:00:00  26116,46594   20326(Klajeyz)/S

SHA256 hash of SKR:
E42A29CCF17BE6EB3BDD1B470A256CD568709867BC6CB0F6E9021E39D1D89A04
>> tonic chambermaid breakup revolver unwind inferno tracker underfoot clockwork tambourine beeswax determine allow carav
an glucose specialist frighten hesitate printer graduate showgirl handiwork ruffled vocalist treadmill aftermath berserk
corporate stairway stupendous pupil alkali <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK41-2020-Q4/ksr-root-2020-q4-0.xml (at Thu Apr 23 18:50:53 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:          H1903017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-07-01T00:00:00 2020-07-22T00:00:00  46594,48903   20326(Klajeyz)/S
2  2020-07-11T00:00:00 2020-08-01T00:00:00  46594         20326(Klajeyz)/S
3  2020-07-21T00:00:00 2020-08-11T00:00:00  46594         20326(Klajeyz)/S
4  2020-07-31T00:00:00 2020-08-21T00:00:00  46594         20326(Klajeyz)/S
5  2020-08-10T00:00:00 2020-08-31T00:00:00  46594         20326(Klajeyz)/S
6  2020-08-20T00:00:00 2020-09-10T00:00:00  46594         20326(Klajeyz)/S
7  2020-08-30T00:00:00 2020-09-20T00:00:00  46594         20326(Klajeyz)/S
8  2020-09-09T00:00:00 2020-09-30T00:00:00  46594         20326(Klajeyz)/S
9  2020-09-19T00:00:00 2020-10-10T00:00:00  26116,46594   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK41-2020-Q4/ksr-root-2020-q4-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-10-01T00:00:00 2020-10-22T00:00:00  26116,46594
2  2020-10-11T00:00:00 2020-11-01T00:00:00  26116
3  2020-10-21T00:00:00 2020-11-11T00:00:00  26116
4  2020-10-31T00:00:00 2020-11-21T00:00:00  26116
5  2020-11-10T00:00:00 2020-12-01T00:00:00  26116
6  2020-11-20T00:00:00 2020-12-11T00:00:00  26116
7  2020-11-30T00:00:00 2020-12-21T00:00:00  26116
8  2020-12-10T00:00:00 2020-12-31T00:00:00  26116
9  2020-12-20T00:00:00 2021-01-10T00:00:00  42351,26116
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
E3068F0CFC5A69CE2C62E12295597607B099D3F1E6C99EB37B6FDBF77FC2F8A1
>> tissue amulet payday article wayside existence gazelle sardonic Burbank gadgetry tempest candidate preclude examine in
verse amusement ruffled nebula stapler vacancy tracker retrospect quiver pocketful kickoff hemisphere suspense voyager lo
ckup repellent Vulcan outfielder <<

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/KSK41-2020-Q4/skr-root-2020-q4-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-10-01T00:00:00 2020-10-22T00:00:00  26116,46594   20326(Klajeyz)/S
2  2020-10-11T00:00:00 2020-11-01T00:00:00  26116         20326(Klajeyz)/S
3  2020-10-21T00:00:00 2020-11-11T00:00:00  26116         20326(Klajeyz)/S
4  2020-10-31T00:00:00 2020-11-21T00:00:00  26116         20326(Klajeyz)/S
5  2020-11-10T00:00:00 2020-12-01T00:00:00  26116         20326(Klajeyz)/S
6  2020-11-20T00:00:00 2020-12-11T00:00:00  26116         20326(Klajeyz)/S
7  2020-11-30T00:00:00 2020-12-21T00:00:00  26116         20326(Klajeyz)/S
8  2020-12-10T00:00:00 2020-12-31T00:00:00  26116         20326(Klajeyz)/S
9  2020-12-20T00:00:00 2021-01-10T00:00:00  26116,42351   20326(Klajeyz)/S

SHA256 hash of SKR:
CDA23C5462D2B4EF1B23D494AF73D68339FB165F85FFF7854C06978DCC39D683
>> spindle Pacific cobra equation flagpole sensation scenic unravel beeswax cannonball steamship molecule rocker hurrican
e stockman Jamaica classroom Wichita backward forever music Yucatan virus leprosy drainage amulet preshrunk microscope sp
igot corporate stockman Jamaica <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
Starting: ksrsigner /media/KSR/KSK41-2021-Q1/ksr-root-2021-q1-0.xml (at Thu Apr 23 18:54:33 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:          H1903017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-10-01T00:00:00 2020-10-22T00:00:00  26116,46594   20326(Klajeyz)/S
2  2020-10-11T00:00:00 2020-11-01T00:00:00  26116         20326(Klajeyz)/S
3  2020-10-21T00:00:00 2020-11-11T00:00:00  26116         20326(Klajeyz)/S
4  2020-10-31T00:00:00 2020-11-21T00:00:00  26116         20326(Klajeyz)/S
5  2020-11-10T00:00:00 2020-12-01T00:00:00  26116         20326(Klajeyz)/S
6  2020-11-20T00:00:00 2020-12-11T00:00:00  26116         20326(Klajeyz)/S
7  2020-11-30T00:00:00 2020-12-21T00:00:00  26116         20326(Klajeyz)/S
8  2020-12-10T00:00:00 2020-12-31T00:00:00  26116         20326(Klajeyz)/S
9  2020-12-20T00:00:00 2021-01-10T00:00:00  26116,42351   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK41-2021-Q1/ksr-root-2021-q1-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-01-01T00:00:00 2021-01-22T00:00:00  42351,26116
2  2021-01-11T00:00:00 2021-02-01T00:00:00  42351
3  2021-01-21T00:00:00 2021-02-11T00:00:00  42351
4  2021-01-31T00:00:00 2021-02-21T00:00:00  42351
5  2021-02-10T00:00:00 2021-03-03T00:00:00  42351
6  2021-02-20T00:00:00 2021-03-13T00:00:00  42351
7  2021-03-02T00:00:00 2021-03-23T00:00:00  42351
8  2021-03-12T00:00:00 2021-04-02T00:00:00  42351
9  2021-03-22T00:00:00 2021-04-12T00:00:00  14631,42351
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
2DD682FF1BDBDC746C1324B663793EB813C1AEDD593F96FF8F3CC819DFE30643
>> button speculate miser Yucatan beeswax suspicious sweatband hydraulic glucose barbecue bluebird potato flatfoot inerti
a concert provincial Aztec recover robust tambourine endow customer prefer Yucatan payday crossover spaniel bottomless ta
lon torpedo afflict decimal <<

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/KSK41-2021-Q1/skr-root-2021-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-01-01T00:00:00 2021-01-22T00:00:00  26116,42351   20326(Klajeyz)/S
2  2021-01-11T00:00:00 2021-02-01T00:00:00  42351         20326(Klajeyz)/S
3  2021-01-21T00:00:00 2021-02-11T00:00:00  42351         20326(Klajeyz)/S
4  2021-01-31T00:00:00 2021-02-21T00:00:00  42351         20326(Klajeyz)/S
5  2021-02-10T00:00:00 2021-03-03T00:00:00  42351         20326(Klajeyz)/S
6  2021-02-20T00:00:00 2021-03-13T00:00:00  42351         20326(Klajeyz)/S
7  2021-03-02T00:00:00 2021-03-23T00:00:00  42351         20326(Klajeyz)/S
8  2021-03-12T00:00:00 2021-04-02T00:00:00  42351         20326(Klajeyz)/S
9  2021-03-22T00:00:00 2021-04-12T00:00:00  42351,14631   20326(Klajeyz)/S

SHA256 hash of SKR:
C0ACD3C7A1D08C9C4E7B92B30FA653FB71594AA19210A15F1DC14C7415113001
>> slowdown penetrate stapler retraction ratchet savagery offload October drifter inferno physique pocketful artist parag
on dwelling Wichita hamlet examine dogsled outfielder physique autopsy ratchet forever Belfast recover drainage hydraulic
 backfield Babylon chairlift adviser <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

Back up the Newly Created SKR

Step	Activity	Initials	Time

25	CA executes the following commands using the terminal window:
	a) List the contents of the KSRFD by executing:
	`ls -ltrR /media/KSR`
	b) Copy the contents of the KSRFD 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 KSRFD by executing:
	`umount /media/KSR`
		JD	19:01

26	CA removes the **KSRFD** containing the SKR files, then gives it to RKOS.	JD	19:01

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
27	CA deactivates the HSM by performing the following steps: **Note: CA will use OP cards not previously utilized in this ceremony if available.** 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 4 of 7 2nd OP card 5 of 7 3rd OP card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	JD	19:04

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
28	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.**	JD	19:05
29	CA places the HSM into a prepared TEB, then seals it.	JD	19:06
30	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. **HSM5W: TEB # BB51184239 / Serial # H1903017**	JD	19:08

Act 4: 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 CO 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 into Tier 5 (Safe Room) to return COs' 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.**	JD	19:10

HSMFD SHA-256 HASH **2020/04/23**

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

 SHA-256:     c41ebb6f36a4d71797fecedb8e8b0f970059b0771214807c00a061e99eb89682
PGP Words:  snowslide Burlington shamrock hemisphere Christmas Pandora stopwatch bookseller
 preshrunk yesteryear spyglass suspicious orca Medusa artist mosquito aardvark examine ruff
led inception atlas belowground merit informant aardvark Orlando fallout ultimate quiver pr
ovincial prefer Istanbul
```

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`	JD	19:10
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 -p` **Note: One copy for audit bundle and one copy for HSMFD package.**	JD	19:11
4	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrR`	JD	19:12
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`	JD	19:12
6	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.	JD	19:13
7	CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: `df`	JD	19:13
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`	JD	19:15
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 -m` b) `umount /media/HSMFD1`	JD	19:15
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.**	JD	19:16
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.**	JD	19:18
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.**	JD	19:19
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.**	JD	19:20
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.**	JD	19:21

```
Script started on Thu Apr 23 18:25:50 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=0.710 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.575 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.692 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.571 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.571/0.637/0.710/0.064 ms
root@coen:/media/HSMFD# ksrsigner /media/Ks\00SR/K\007SK41-2020-Q3/ks\007r-root-2020-q3-0
.xml
Starting: ksrsigner /media/KSR/KSK41-2020-Q3/ksr-root-2020-q3-0.xml (at Thu Apr 23 18:42:
08 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:         H1903017

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

Validate and Process KSR /media/KSR/KSK41-2020-Q3/ksr-root-2020-q3-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-07-01T00:00:00 2020-07-22T00:00:00  46594,48903
2  2020-07-11T00:00:00 2020-08-01T00:00:00  46594
3  2020-07-21T00:00:00 2020-08-11T00:00:00  46594
4  2020-07-31T00:00:00 2020-08-21T00:00:00  46594
5  2020-08-10T00:00:00 2020-08-31T00:00:00  46594
6  2020-08-20T00:00:00 2020-09-10T00:00:00  46594
7  2020-08-30T00:00:00 2020-09-20T00:00:00  46594
8  2020-09-09T00:00:00 2020-09-30T00:00:00  46594
9  2020-09-19T00:00:00 2020-10-10T00:00:00  26116,46594
...PASSED.

SHA256 hash of KSR:
7B5188B568B4E932D9AC26DFB04D28ADBC09D70F186BAFCC2FF067718BF9B973
>> kickoff enchanting newborn positive frighten politeness treadmill component sugar pene
trate bookshelf therapist merit disruptive breadline perceptive showgirl applicant stopwa
tch atmosphere beaming Hamilton rocker revolver cement upcoming freedom hideaway obtuse W
aterloo sentence hurricane <<
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/KSK41-2020-Q3/skr-root-2020-q3-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-07-01T00:00:00 2020-07-22T00:00:00  46594,48903  20326(Klajeyz)/S
2  2020-07-11T00:00:00 2020-08-01T00:00:00  46594        20326(Klajeyz)/S
3  2020-07-21T00:00:00 2020-08-11T00:00:00  46594        20326(Klajeyz)/S
4  2020-07-31T00:00:00 2020-08-21T00:00:00  46594        20326(Klajeyz)/S
5  2020-08-10T00:00:00 2020-08-31T00:00:00  46594        20326(Klajeyz)/S
6  2020-08-20T00:00:00 2020-09-10T00:00:00  46594        20326(Klajeyz)/S
7  2020-08-30T00:00:00 2020-09-20T00:00:00  46594        20326(Klajeyz)/S
8  2020-09-09T00:00:00 2020-09-30T00:00:00  46594        20326(Klajeyz)/S
9  2020-09-19T00:00:00 2020-10-10T00:00:00  26116,46594  20326(Klajeyz)/S

SHA256 hash of SKR:
E42A29CCF17BE6EB3BDD1B470A256CD568709867BC6CB0F6E9021E39D1D89A04
>> tonic chambermaid breakup revolver unwind inferno tracker underfoot clockwork tambouri
ne beeswax determine allow caravan glucose specialist frighten hesitate printer graduate
showgirl handiwork ruffled vocalist treadmill aftermath berserk corporate stairway stupen
dous pupil alkali <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20200423-184208.log **********
root@coen:/media/HSMFD# cp /media/KSR/K\007SK41-2020-Q3/ks\007r\007-root-2020-q3-0.xml /m
edia/KSR/Ks007SK41-2020-Q3/s
root@coen:/media/HSMFD# ksrsigner /media/KSR/KS\007K41-2020\007-Q4/ks\007r-root-2020-q4-0
.xml
Starting: ksrsigner /media/KSR/KSK41-2020-Q4/ksr-root-2020-q4-0.xml (at Thu Apr 23 18:50:
53 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:         H1903017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2020-07-01T00:00:00 2020-07-22T00:00:00  46594,48903  20326(Klajeyz)/S
2  2020-07-11T00:00:00 2020-08-01T00:00:00  46594        20326(Klajeyz)/S
3  2020-07-21T00:00:00 2020-08-11T00:00:00  46594        20326(Klajeyz)/S
4  2020-07-31T00:00:00 2020-08-21T00:00:00  46594        20326(Klajeyz)/S
```

```
5  2020-08-10T00:00:00 2020-08-31T00:00:00  46594          20326(Klajeyz)/S
6  2020-08-20T00:00:00 2020-09-10T00:00:00  46594          20326(Klajeyz)/S
7  2020-08-30T00:00:00 2020-09-20T00:00:00  46594          20326(Klajeyz)/S
8  2020-09-09T00:00:00 2020-09-30T00:00:00  46594          20326(Klajeyz)/S
9  2020-09-19T00:00:00 2020-10-10T00:00:00  26116,46594    20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK41-2020-Q4/ksr-root-2020-q4-0.xml...
#  Inception           Expiration          ZSK Tags       KSK Tag(CKA_LABEL)
1  2020-10-01T00:00:00 2020-10-22T00:00:00  26116,46594
2  2020-10-11T00:00:00 2020-11-01T00:00:00  26116
3  2020-10-21T00:00:00 2020-11-11T00:00:00  26116
4  2020-10-31T00:00:00 2020-11-21T00:00:00  26116
5  2020-11-10T00:00:00 2020-12-01T00:00:00  26116
6  2020-11-20T00:00:00 2020-12-11T00:00:00  26116
7  2020-11-30T00:00:00 2020-12-21T00:00:00  26116
8  2020-12-10T00:00:00 2020-12-31T00:00:00  26116
9  2020-12-20T00:00:00 2021-01-10T00:00:00  42351,26116
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
E3068F0CFC5A69CE2C62E12295597607B099D3F1E6C99EB37B6FDBF77FC2F8A1
>> tissue amulet payday article wayside existence gazelle sardonic Burbank gadgetry tempe
st candidate preclude examine inverse amusement ruffled nebula stapler vacancy tracker re
trospect quiver pocketful kickoff hemisphere suspense voyager lockup repellent Vulcan out
fielder <<
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/KSK41-2020-Q4/skr-root-2020-q4-0.xml
#  Inception           Expiration          ZSK Tags       KSK Tag(CKA_LABEL)
1  2020-10-01T00:00:00 2020-10-22T00:00:00  26116,46594    20326(Klajeyz)/S
2  2020-10-11T00:00:00 2020-11-01T00:00:00  26116          20326(Klajeyz)/S
3  2020-10-21T00:00:00 2020-11-11T00:00:00  26116          20326(Klajeyz)/S
4  2020-10-31T00:00:00 2020-11-21T00:00:00  26116          20326(Klajeyz)/S
5  2020-11-10T00:00:00 2020-12-01T00:00:00  26116          20326(Klajeyz)/S
6  2020-11-20T00:00:00 2020-12-11T00:00:00  26116          20326(Klajeyz)/S
7  2020-11-30T00:00:00 2020-12-21T00:00:00  26116          20326(Klajeyz)/S
8  2020-12-10T00:00:00 2020-12-31T00:00:00  26116          20326(Klajeyz)/S
9  2020-12-20T00:00:00 2021-01-10T00:00:00  26116,42351    20326(Klajeyz)/S

SHA256 hash of SKR:
CDA23C5462D2B4EF1B23D494AF73D68339FB165F85FFF7854C06978DCC39D683
>> spindle Pacific cobra equation flagpole sensation scenic unravel beeswax cannonball st
eamship molecule rocker hurricane stockman Jamaica classroom Wichita backward forever mus
ic Yucatan virus leprosy drainage amulet preshrunk microscope spigot corporate stockman J
amaica <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20200423-185053.log **********
root@coen:/media/HSMFD# cp /media/KSR/KSK007SK41-2020-Q4/skr\007-root-2020-q4-0.xml /med
ia/KSR/KS\007K41-2021-Q1/s
root@coen:/media/HSMFD# ksrsigner /media/KSR/K\007SK41-2021-Q1/ksr-root-2021-q1-0.xml
Starting: ksrsigner /media/KSR/KSK41-2021-Q1/ksr-root-2021-q1-0.xml (at Thu Apr 23 18:54:
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:         H1903017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags       KSK Tag(CKA_LABEL)
1  2020-10-01T00:00:00 2020-10-22T00:00:00  26116,46594    20326(Klajeyz)/S
2  2020-10-11T00:00:00 2020-11-01T00:00:00  26116          20326(Klajeyz)/S
3  2020-10-21T00:00:00 2020-11-11T00:00:00  26116          20326(Klajeyz)/S
4  2020-10-31T00:00:00 2020-11-21T00:00:00  26116          20326(Klajeyz)/S
5  2020-11-10T00:00:00 2020-12-01T00:00:00  26116          20326(Klajeyz)/S
6  2020-11-20T00:00:00 2020-12-11T00:00:00  26116          20326(Klajeyz)/S
7  2020-11-30T00:00:00 2020-12-21T00:00:00  26116          20326(Klajeyz)/S
8  2020-12-10T00:00:00 2020-12-31T00:00:00  26116          20326(Klajeyz)/S
9  2020-12-20T00:00:00 2021-01-10T00:00:00  26116,42351    20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK41-2021-Q1/ksr-root-2021-q1-0.xml...
#  Inception           Expiration          ZSK Tags       KSK Tag(CKA_LABEL)
1  2021-01-01T00:00:00 2021-01-22T00:00:00  42351,26116
2  2021-01-11T00:00:00 2021-02-01T00:00:00  42351
3  2021-01-21T00:00:00 2021-02-11T00:00:00  42351
4  2021-01-31T00:00:00 2021-02-21T00:00:00  42351
5  2021-02-10T00:00:00 2021-03-03T00:00:00  42351
6  2021-02-20T00:00:00 2021-03-13T00:00:00  42351
7  2021-03-02T00:00:00 2021-03-23T00:00:00  42351
8  2021-03-12T00:00:00 2021-04-02T00:00:00  42351
9  2021-03-22T00:00:00 2021-04-12T00:00:00  14631,42351
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
```

```
2DD582FF1BDBDC746C1324B663793EB813C1AEDD593F96FF8F3CC819DFE30643
>> button speculate miser Yucatan beeswax suspicious sweatband hydraulic glucose barbecue
 bluebird potato flatfoot inertia concert provincial Aztec recover robust tambourine endo
w customer prefer Yucatan payday crossover spaniel bottomless talon torpedo afflict decim
al <<
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/KSK41-2021-Q1/skr-root-2021-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-01-01T00:00:00 2021-01-22T00:00:00  26116,42351   20326(Klajeyz)/S
2  2021-01-11T00:00:00 2021-02-01T00:00:00  42351         20326(Klajeyz)/S
3  2021-01-21T00:00:00 2021-02-11T00:00:00  42351         20326(Klajeyz)/S
4  2021-01-31T00:00:00 2021-02-21T00:00:00  42351         20326(Klajeyz)/S
5  2021-02-10T00:00:00 2021-03-03T00:00:00  42351         20326(Klajeyz)/S
6  2021-02-20T00:00:00 2021-03-13T00:00:00  42351         20326(Klajeyz)/S
7  2021-03-02T00:00:00 2021-03-23T00:00:00  42351         20326(Klajeyz)/S
8  2021-03-12T00:00:00 2021-04-02T00:00:00  42351         20326(Klajeyz)/S
9  2021-03-22T00:00:00 2021-04-12T00:00:00  42351,14631   20326(Klajeyz)/S

SHA256 hash of SKR:
C0ACD3C7A1D08C9C4E7B92B30FA653FB71594AA19210A15F1DC14C7415113001
>> slowdown penetrate stapler retraction ratchet savagery offload October drifter inferno
 physique pocketful artist paragon dwelling Wichita hamlet examine dogsled outfielder phy
sique autopsy ratchet forever Belfast recover drainage hydraulic backfield Babylon chairl
ift adviser <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20200423-185433.log **********
root@coen:/media/HSMFD# lpadmin -p HP -o copies-default=3
root@coen:/media/HSMFD# for i in $(ls -1 ksrsigner-202004*.log); do printlog $i; done
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /media/KSR/
/media/KSR/:
total 48
drwxr-xr-x 2 root root 16384 Apr 23 18:47 \033[0m\033[01;34mKSK41-2020-Q3\033[0m
drwxr-xr-x 2 root root 16384 Apr 23 18:52 \033[01;34mKSK41-2020-Q4\033[0m
drwxr-xr-x 2 root root 16384 Apr 23 18:56 \033[01;34mKSK41-2021-Q1\033[0m

/media/KSR/KSK41-2020-Q3:
total 144
-rw-r--r-- 1 root root 20369 Apr 22 04:42 skr.xml.20200423184208
-rw-r--r-- 1 root root 19600 Apr 22 04:42 ksr-root-2020-q3-0.xml
-rw-r--r-- 1 root root  1148 Apr 22 04:42 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 18:47 skr.xml
-rw-r--r-- 1 root root 20369 Apr 23 18:47 skr-root-2020-q3-0.xml

/media/KSR/KSK41-2020-Q4:
total 144
-rw-r--r-- 1 root root 19600 Apr 22 04:42 ksr-root-2020-q4-0.xml
-rw-r--r-- 1 root root  1148 Apr 22 04:42 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 18:49 skr.xml.20200423185053
-rw-r--r-- 1 root root 20369 Apr 23 18:52 skr.xml
-rw-r--r-- 1 root root 20369 Apr 23 18:52 skr-root-2020-q4-0.xml

/media/KSR/KSK41-2021-Q1:
total 144
-rw-r--r-- 1 root root 19600 Apr 22 04:42 ksr-root-2021-q1-0.xml
-rw-r--r-- 1 root root  1148 Apr 22 04:42 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 18:54 skr.xml.20200423185433
-rw-r--r-- 1 root root 20369 Apr 23 18:56 skr.xml
-rw-r--r-- 1 root root 20369 Apr 23 18:56 skr-root-2021-q1-0.xml
root@coen:/media/HSMFD# cp -pR /media/KSR/* .
root@coen:/media/HSMFD# ls -ltrR
.:
total 3096
-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  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
-rw-r--r-- 1 root root 12174 Feb 16 02:34 ttyaudit-ttyS0-20200216-020929.log
-rw-r--r-- 1 root root 23671 Feb 16 02:38 script-20200216.log
-rw-r--r-- 1 root root  6308 Apr 23 18:47 ksrsigner-20200423-184208.log
drwxr-xr-x 2 root root  8192 Apr 23 18:47 \033[01;34mKSK41-2020-Q3\033[0m
-rw-r--r-- 1 root root  7151 Apr 23 18:52 ksrsigner-20200423-185053.log
drwxr-xr-x 2 root root  8192 Apr 23 18:52 \033[01;34mKSK41-2020-Q4\033[0m
-rw-r--r-- 1 root root 14325 Apr 23 18:56 ttyaudit-ttyS0-20200423-182706.log
drwxr-xr-x 2 root root  8192 Apr 23 18:56 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root  7151 Apr 23 18:56 ksrsigner-20200423-185433.log
drwxr-xr-x 2 root root  8192 Apr 23 18:56 \033[01;34mKSK41-2021-Q1\033[0m
```

```
-rw-r--r-- 1 root root  16384 Apr 23 18:59 script-20200423.log

./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

./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

./KSK41-2020-Q3:
total 104
-rw-r--r-- 1 root root 20369 Apr 22 04:42 skr.xml.20200423184208
-rw-r--r-- 1 root root 19600 Apr 22 04:42 ksr-root-2020-q3-0.xml
-rw-r--r-- 1 root root  1148 Apr 22 04:42 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 18:47 skr.xml
```

```
-rw-r--r-- 1 root root 20369 Apr 23 18:47 skr-root-2020-q3-0.xml

./KSK41-2020-Q4:
total 104
-rw-r--r-- 1 root root 19600 Apr 22 04:42 ksr-root-2020-q4-0.xml
-rw-r--r-- 1 root root  1148 Apr 22 04:42 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 18:49 skr.xml.20200423185053
-rw-r--r-- 1 root root 20369 Apr 23 18:52 skr.xml
-rw-r--r-- 1 root root 20369 Apr 23 18:52 skr-root-2020-q4-0.xml

./tmp:
total 72
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Apr 23 18:56 skr.keybundle.0
-rw-r--r-- 1 root root 1768 Apr 23 18:56 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Apr 23 18:56 skr.keybundle.3

./KSK41-2021-Q1:
total 104
-rw-r--r-- 1 root root 19600 Apr 22 04:42 ksr-root-2021-q1-0.xml
-rw-r--r-- 1 root root  1148 Apr 22 04:42 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 18:54 skr.xml.20200423185433
-rw-r--r-- 1 root root 20369 Apr 23 18:56 skr.xml
-rw-r--r-- 1 root root 20369 Apr 23 18:56 skr-root-2021-q1-0.xml
root@coen:/media/HSMFD# umount /media/KSR/
root@coen:/media/HSMFD# exit
exit

Script done on Thu Apr 23 19:10:04 2020
```

```
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   H1903017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   BBL CRC32: 0xDBC9B9F2
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   Running applicationBootLoader at 0xEFDC0000
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   H1903017 011403 ABL 030 : Tamper Challenge Response Key
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   ABL CRC32: 0xE7E0FA6A
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   ####################################
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   ###     ABL tamper records       ###
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   ####################################
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   ====================================
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   vextoosTamperCount:     0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   vintoosTamperCount:     5
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   vbboosTamperCount:      0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   maxstrtempTamperCount:  0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   minstrtempTamperCount:  0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   meshTamperCount:        0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   extampSMKTamperCount:   0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   extampIMKTamperCount:   0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   tempdiffTamperCount:    0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   pfTamperCount:          5
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   restartTamperCount:     16
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   Current tamper bitmaps:
2020-04-23T18:29:05+0000        ttyS0   ======================
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
```

```
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   Bitmapped Change Record (most recent first):
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0   ============================================
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:05+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0   Running cryptoApplication at 0xEBF00000
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0   Jumping to startup @ 0x001037B4
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0   Board is P2020RDB
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0   board_smp_init: 2 cpu
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:07+0000        ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2020-04-23T18:29:07+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0   Starting next program at v0015183c
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0   Starting K-Series Kernel
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0   Copyright Ultra Electronics AEP. All Rights Reserved.
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0   Sat Jan  9 04:45:17 1971
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:08+0000        ttyS0   Starting auditd v2.0 ... started.
2020-04-23T18:29:08+0000        ttyS0
2020-04-23T18:29:09+0000        ttyS0   Interface 0 configured for IPv6.
2020-04-23T18:29:09+0000        ttyS0
2020-04-23T18:29:09+0000        ttyS0   Interface 0 configured for IPv4.
2020-04-23T18:29:09+0000        ttyS0
2020-04-23T18:29:09+0000        ttyS0   Interface 1 configured for IPv6.
2020-04-23T18:29:09+0000        ttyS0
2020-04-23T18:29:09+0000        ttyS0   Interface 1 configured for IPv4.
2020-04-23T18:29:09+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0   route: writing to routing socket: Network is unreachable
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0   add net default: gateway ::: Network is unreachable
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0   route: writing to routing socket: Network is unreachable
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0   Starting USB driver...
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0   9860 v3.4 Keyper Application - May 19 2017 15:48:58
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0
2020-04-23T18:29:10+0000        ttyS0
```

```
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running DES POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   DES POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running Triple DES POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Triple DES POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running AES POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   AES POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running SHA1 POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   SHA1 POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running SHA2 POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   SHA2 POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running RandomGen POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   RandomGen POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running RSA POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   RSA POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running DSA POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   DSA POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running SEED POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   SEED POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running RIPEMD160 POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   RIPEMD160 POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running ECC POST Test
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   ECC POST Test Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Running HMAC POST Tests
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   HMAC POST Tests Passed
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0   Audit on 9/1/1971 04:45:20 00100008
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:12+0000        ttyS0
```

```
2020-04-23T18:29:12+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Keyper 9860-2  Serial Number H1903017
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Memory Usage:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   RAM (free/total)        192Mb/256Mb
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Flash (free/total)      128Mb/128Mb
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0      black store          524b
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0      statistics           112b
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0      other                116b
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   RedStore (free/total)   107Kb/128Kb
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Network Configuration:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Interface 0:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0       IPv4: enabled
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0       IPv6: enabled
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C4:9A / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c49a/64
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Interface 1:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0       IPv4: enabled
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0       IPv6: enabled
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C4:9B / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c49b/64
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   HSM Port 0: 05000
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   HSM Port 1: 03000
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Default Gateway(s): 0.0.0.0 ::
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Software Versions:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   BBL 030 ABL 021 App 034
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   CPLD Version:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   1.9
2020-04-23T18:29:13+0000        ttyS0
```

```
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   SCR Firmware Version:
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   OROS-R2.99-R1.20
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   HmcListener: Created IPv4 socket 12 on port 3000.
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   HmcListener: Created IPv6 socket 13 on port 3000.
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:29:13+0000        ttyS0   Audit on 9/1/1971 04:45:21 00100003
2020-04-23T18:29:13+0000        ttyS0
2020-04-23T18:35:33+0000        ttyS0   Audit on 9/1/1971 04:51:41 0020006a
2020-04-23T18:35:33+0000        ttyS0
2020-04-23T18:35:54+0000        ttyS0   Audit on 9/1/1971 04:52:02 0020006a
2020-04-23T18:35:54+0000        ttyS0
2020-04-23T18:36:30+0000        ttyS0   Audit on 9/1/1971 04:52:38 00200069 0A400000B686296E
2020-04-23T18:36:30+0000        ttyS0
2020-04-23T18:36:59+0000        ttyS0   Audit on 9/1/1971 04:53:08 00200069 0A4000009D86296E
2020-04-23T18:36:59+0000        ttyS0
2020-04-23T18:37:33+0000        ttyS0   Audit on 9/1/1971 04:53:40 00200069 0A4000009DC6296E
2020-04-23T18:37:33+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0   TcpListener: Created IPv4 socket 19 on port 5000.
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0   TcpListener: Created IPv6 socket 20 on port 5000.
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:37:35+0000        ttyS0   Audit on 9/1/1971 04:53:44 00100002
2020-04-23T18:37:35+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0   TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0   CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:42:21+0000        ttyS0   TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2020-04-23T18:42:21+0000        ttyS0
2020-04-23T18:47:48+0000        ttyS0
2020-04-23T18:47:48+0000        ttyS0
2020-04-23T18:47:48+0000        ttyS0   CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2020-04-23T18:47:48+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0   TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
```

```
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0   CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:51:07+0000        ttyS0   TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2020-04-23T18:51:07+0000        ttyS0
2020-04-23T18:52:52+0000        ttyS0
2020-04-23T18:52:52+0000        ttyS0
2020-04-23T18:52:52+0000        ttyS0   CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2020-04-23T18:52:52+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0   TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0   CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:54:46+0000        ttyS0   TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2020-04-23T18:54:46+0000        ttyS0
2020-04-23T18:56:11+0000        ttyS0
2020-04-23T18:56:11+0000        ttyS0
2020-04-23T18:56:11+0000        ttyS0   CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2020-04-23T18:56:11+0000        ttyS0
2020-04-23T19:03:07+0000        ttyS0   Audit on 9/1/1971 05:19:15 00200069 0A400000B686296E
2020-04-23T19:03:07+0000        ttyS0
2020-04-23T19:03:36+0000        ttyS0   Audit on 9/1/1971 05:19:44 00200069 0A4000009D86296E
2020-04-23T19:03:36+0000        ttyS0
2020-04-23T19:04:01+0000        ttyS0   Audit on 9/1/1971 05:20:09 00200069 0A4000009DC6296E
2020-04-23T19:04:01+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0   TcpListener: Closed IPv4 socket 19 on port 5000.
2020-04-23T19:04:07+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0   TcpListener: Closed IPv6 socket 20 on port 5000.
2020-04-23T19:04:07+0000        ttyS0
2020-04-23T19:04:07+0000        ttyS0   Audit on 9/1/1971 05:20:15 00100003
2020-04-23T19:04:07+0000        ttyS0
```

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-202004*.log` c) `enscript -Gr --font="Courier8" ttyaudit-tty*-202004*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**	JD	19:25

Place HSMFDs and OS DVDs into a TEB

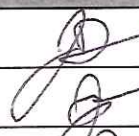
Step	Activity	Initials	Time
16	CA executes the following commands using the terminal window to unmount the HSMFD: a) `cd /tmp` b) `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder.	JD	19:25
17	CA performs the following steps to switch OFF the laptop and remove the OS DVD: a) Remove the OS DVD from the laptop. b) Turn OFF the laptop by pressing the power button. c) Disconnect all connections from the laptop.	JD	19:26
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.	JD	19:28
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 # BB91951384**	JD	19:29
20	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	JD	19:29

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.	JD	19:31
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. **Laptop3: TEB # BB81420121 / Service Tag # C8SVSG2**	JD	19:32

Place Crypto Officer Credentials into TEBs

Step	Activity	Initials	Time
23	CA perform the following steps sequentially for the COs listed below: a) Gather the OP TEB and plastic case prepared for the CO. b) Take the CO's OP card from the card holder and place it inside of the plastic case. c) Place the plastic case into the prepared TEB, read aloud the TEB number and description, then seal it. d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory. e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. f) IW writes the date and time, then signs the table of IW's script, then CA initials the entry. g) IW places the TEBs on the ceremony table. h) Repeat steps for the remaining COs' credentials on the list. **CO4: Carlos Martinez** **OP TEB # BB91951363** **CO5: Olafur Gudmundsson** **OP TEB # BB91951362** **CO6: Nicolas Antoniello** **OP TEB # BB91951361**	JD	19:41

CO	Card Type	TEB #	Printed Name	Signature	Date	Time	CA Initials
CO4	OP 4 of 7	OP TEB # BB91951363	Jonathan Denison		2020 Apr 23	19:36	FA
CO5	OP 5 of 7	OP TEB # BB91951362	Jonathan Denison		2020 Apr 23	19:39	FA
CO6	OP 6 of 7	OP TEB # BB91951361	Jonathan Denison		2020 Apr 23	19:41	FA

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.)	JD	19:42
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.**	JD	19:43
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.**	JD	19:44
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. **HSM5W: TEB # BB51184239** **Laptop3: TEB # BB81420121** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384**	JD	19:47

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.	JD	19:47
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.	JD	19:48
30	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	JD	19:48

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
31	CA and IW transport a flashlight, and escort SSC2 into Tier 5 (Safe Room.)	JD	19:49
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.**	JD	19:51
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.**	JD	19:51

Return Crypto Officer Credentials to Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
34	IW performs the following steps sequentially to return the required TEBs: a) IW reads aloud the TEB number, then verifies the integrity of the TEB while showing it to the audit camera above b) After the CA operates the guard key in the bottom lock, IW uses the CO's tenant key to operate the top lock and opens the CO's safe deposit box. c) IW reads aloud the safe deposit box number, places the TEB inside, then closes and locks the safe deposit box with assistance from the CA. d) IW writes the date and time, then signs the safe log where **"Return"** is indicated. e) CA verifies the completed safe log entry, then initials it. **CO4: Carlos Martinez** **Box # 1068** **OP TEB # BB91951363** **CO5: Olafur Gudmundsson** **Box # 1789** **OP TEB # BB91951362** **CO6: Nicolas Antoniello** **Box # 1073** **OP TEB # BB91951361**	JD	19:59

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.	JD	19:59
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.	JD	20:00
37	CA, IW, and SSC2 leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	JD	20:00

Place Crypto Officer Keys into TEBs

Step	Activity	Initials	Time
38	CA performs the following steps sequentially for the COs key listed below: a) Gather the CO key TEB and envelope prepared for the CO. b) IW gives the CO key to CA who then places it inside of the envelope. c) Place the envelope into the prepared TEB, read aloud the TEB number and description, then seal it. d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory. e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. f) Repeat steps for remaining COs' keys on the list. **CO4: Carlos Martinez** **Key TEB # BB91951358** **CO5: Olafur Gudmundsson** **Key TEB # BB91951359** **CO6: Nicolas Antoniello** **Key TEB # BB91951360** **Note: The COs' keys will be promptly returned to the COs who will sign a second key declaration form confirming receipt. The completed declaration forms will be available on the IANA web page along with the standard post-ceremony materials.**	JD	20:11

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Carlos Martinez** hereby attest that my safe deposit box key for safe deposit box **#1068** located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951284** before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into **TEB #BB91951358** before the key was returned to me.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name CARLOS MARTÍNEZ

Signature Carlos Martinez

Date 29/04/2020 (April 29, 2020)

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Olafur Gudmundsson** hereby attest that my safe deposit box key for safe deposit box **#1789** located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951277** before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into **TEB #BB91951359** before the key was returned to me.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name ÓLAFUR GUÐMUNDSSON

Signature 

Date 2020/4/27

Crypto Officer Safe Deposit Box Key Declaration

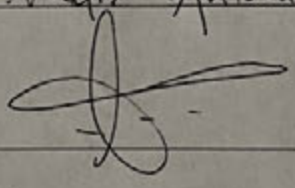
Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Nicolas Antoniello** hereby attest that my safe deposit box key for safe deposit box **#1073** located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951289** before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into **TEB #BB91951360** before the key was returned to me.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name Nicolas Antoniello

Signature 

Date 4/27/2020

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Joao Luis Silva Damas** hereby attest that my safe deposit box key for safe deposit box **#1069** located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951281** before transmitting the key via courier.

If the key was used in the ceremony, I witnessed its extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization remotely when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into **TEB #NULL** before the key was returned to me. AS MY KEY WAS NOT USED IN THIS KSK CEREMONY IT WAS RETURNED TO ME IN THE SAME ORIGINAL TEB BAG THAT I SENT IT IN.

I attest the safe deposit box key was returned to me with no indication of tamper evidence, and to the best of my knowledge the chain of custody of my safe deposit box key was protected and maintained for the period that it was outside of my possession.

Printed Name JOAO LUIS SILVA DAMAS

Signature J. L DA

Date 27-APRIL-2020

Act 5: Close the Key Signing Ceremony

The CA will finish the ceremony by performing the following steps:

- Read any exceptions that occurred during the ceremony
- Call the ceremony participants to sign the IW's script
- Stop the online streaming and video recording
- Ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Prepare the audit bundle materials

Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.	JD	20:11
2	CA asks any COs who are participating remotely if they have any concerns pertaining to the ceremony or exceptions which may have occurred.	JD	20:12
3	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. **All signatories declare that this script is a true and accurate record of the ceremony.**	JD	20:13
4	CA reviews IW's script, then signs the participants list.	JD	20:16
5	IW signs the list and records the completion time.	JD	20:16

Stop Online Streaming and Post Ceremony Information

Step	Activity	Initials	Time
6	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.	JD	20:17
7	CA informs onsite participants of post ceremony activities.	JD	20:17
8	Ceremony participants take a group photo.	JD	20:20
9	CA acknowledges the participation of the COs, RZM, and Auditors in the call, then stops the call.	JD	20:21

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

Step	Activity	Initials	Time
10	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.)	JD	20:31
11	CA requests that an SA stop the audit camera video recording.	JD	20:31

Bundle Audit Materials

Step	Activity	Initials	Time
12	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: **20200216 00:00:00 to 20200424 00:00:00 UTC** e) IW's attestation (See Appendix C on page 32). f) SA's attestation (See Appendix D on page 33 and Appendix E on page 34). All TEBs are labeled **Root DNSSEC KSK Ceremony 41**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	JD	2117

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`
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 on page 32.

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 on page 33.

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 on page 34. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

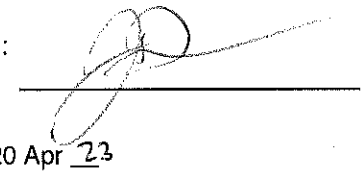
7. Other items

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: **Jonathan Denison**

Signature: 

Date: 2020 Apr 23

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:

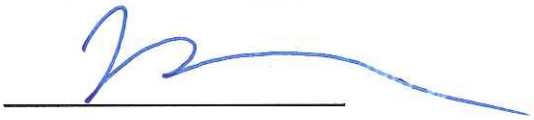
a) There were NO discrepancies found on the system configurations, assigned authorizations and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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: **20200216 00:00:00 to 20200424 00:00:00 UTC.**

SA: Patrick Tudor

Signature: 

Date: 2020 Apr 23

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 5th Edition (2020-04-07). There are no part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

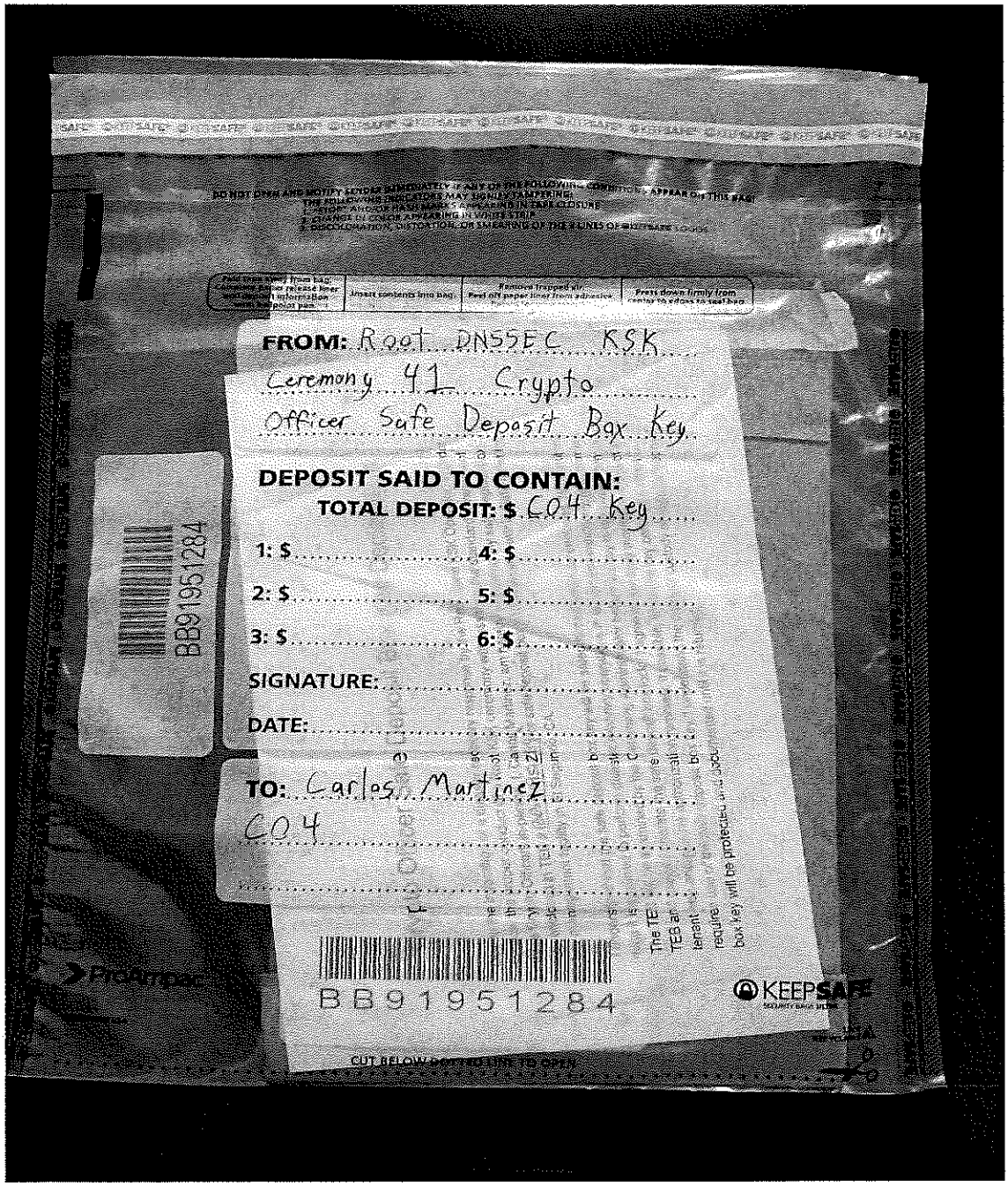
SA: PATRICK TUDOR

Signature: 

Date: 2020 Apr 23

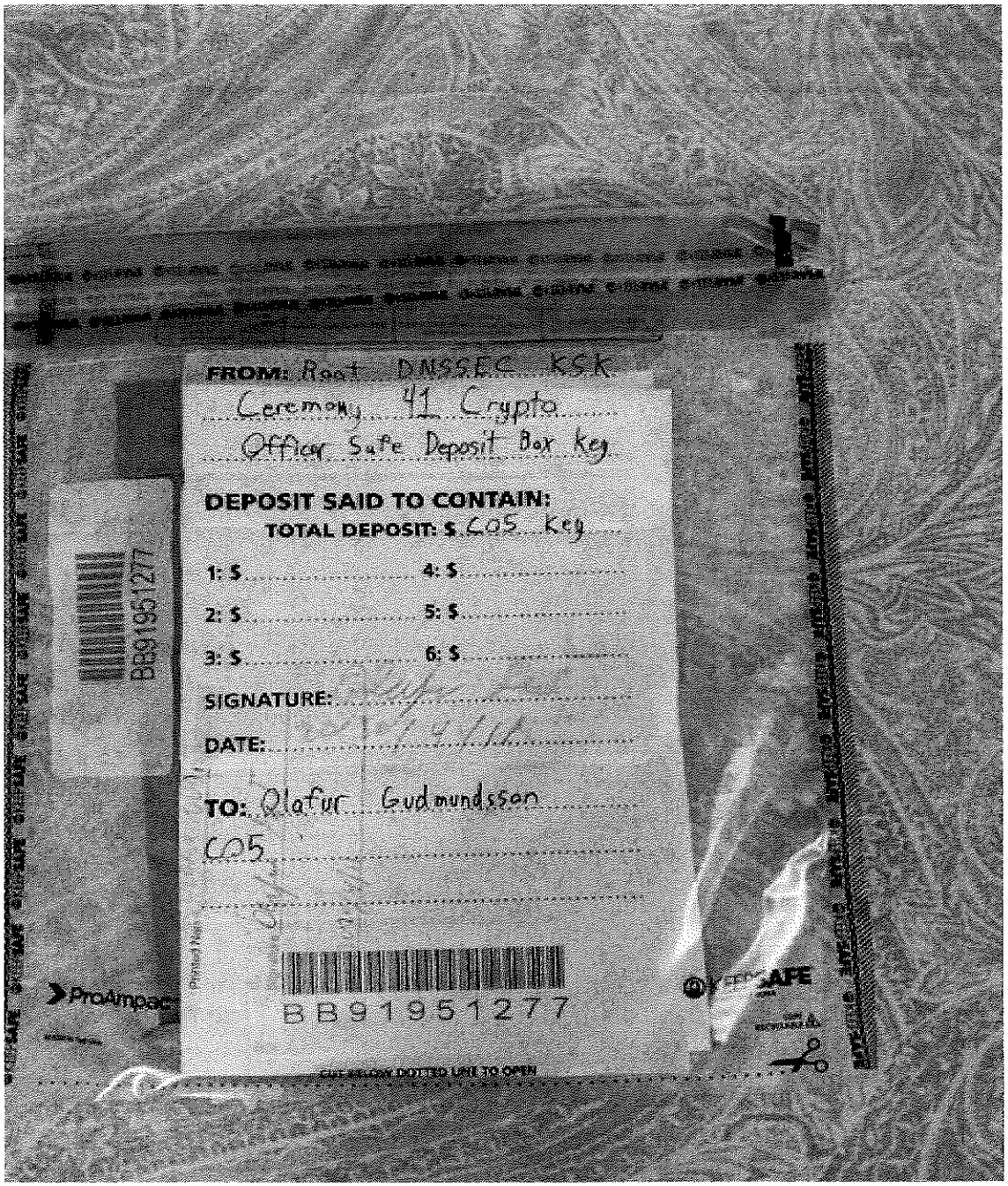
Appendix F: CO4 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO4 Carlos Martinez** Safe Deposit Box **Key TEB # BB91951284** dispatched from the CO.



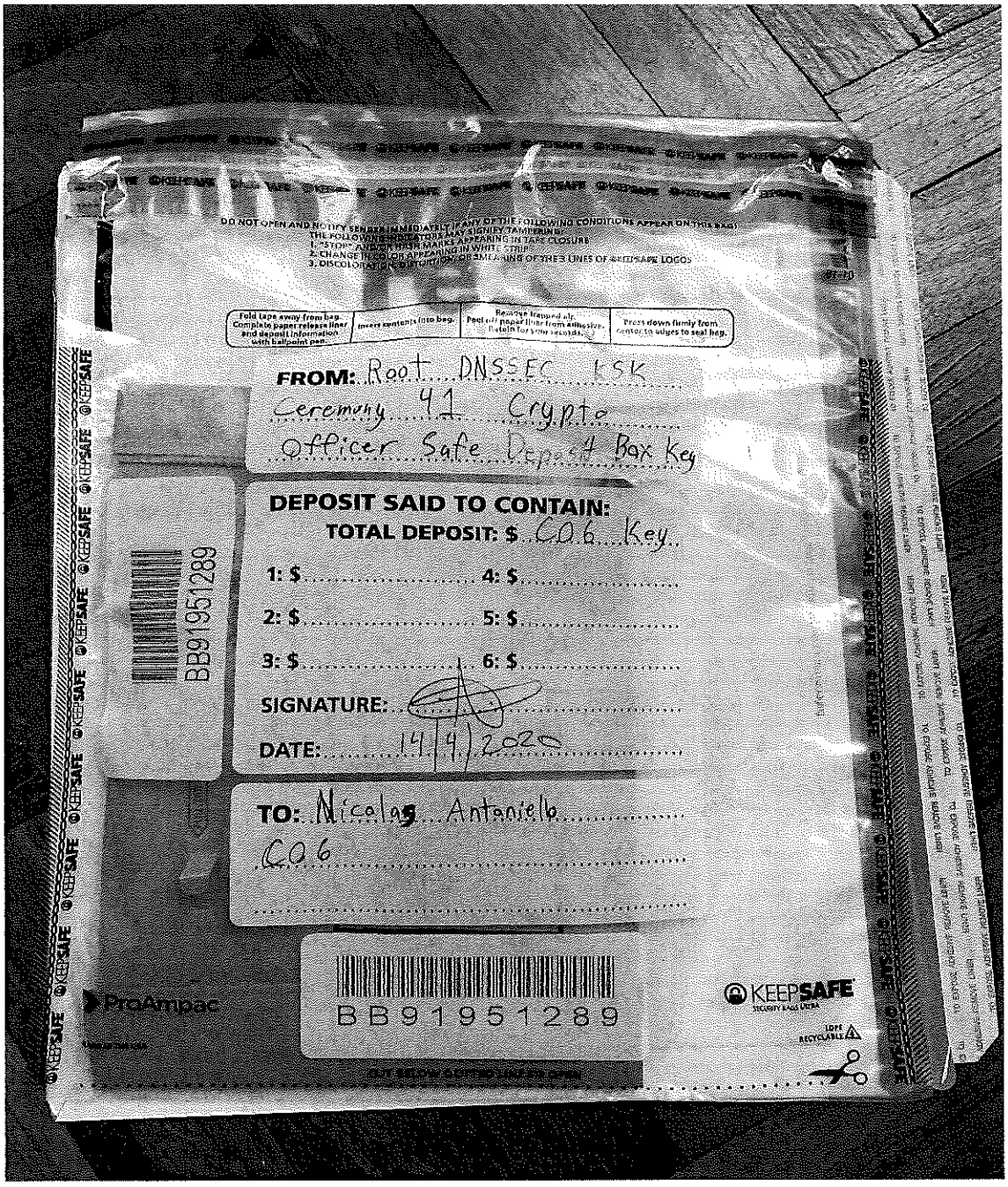
Appendix G: CO5 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO5 Olafur Gudmundsson** Safe Deposit Box **Key TEB # BB91951277** dispatched from the CO.



Appendix H: CO6 Safe Deposit Box Key Chain of Custody

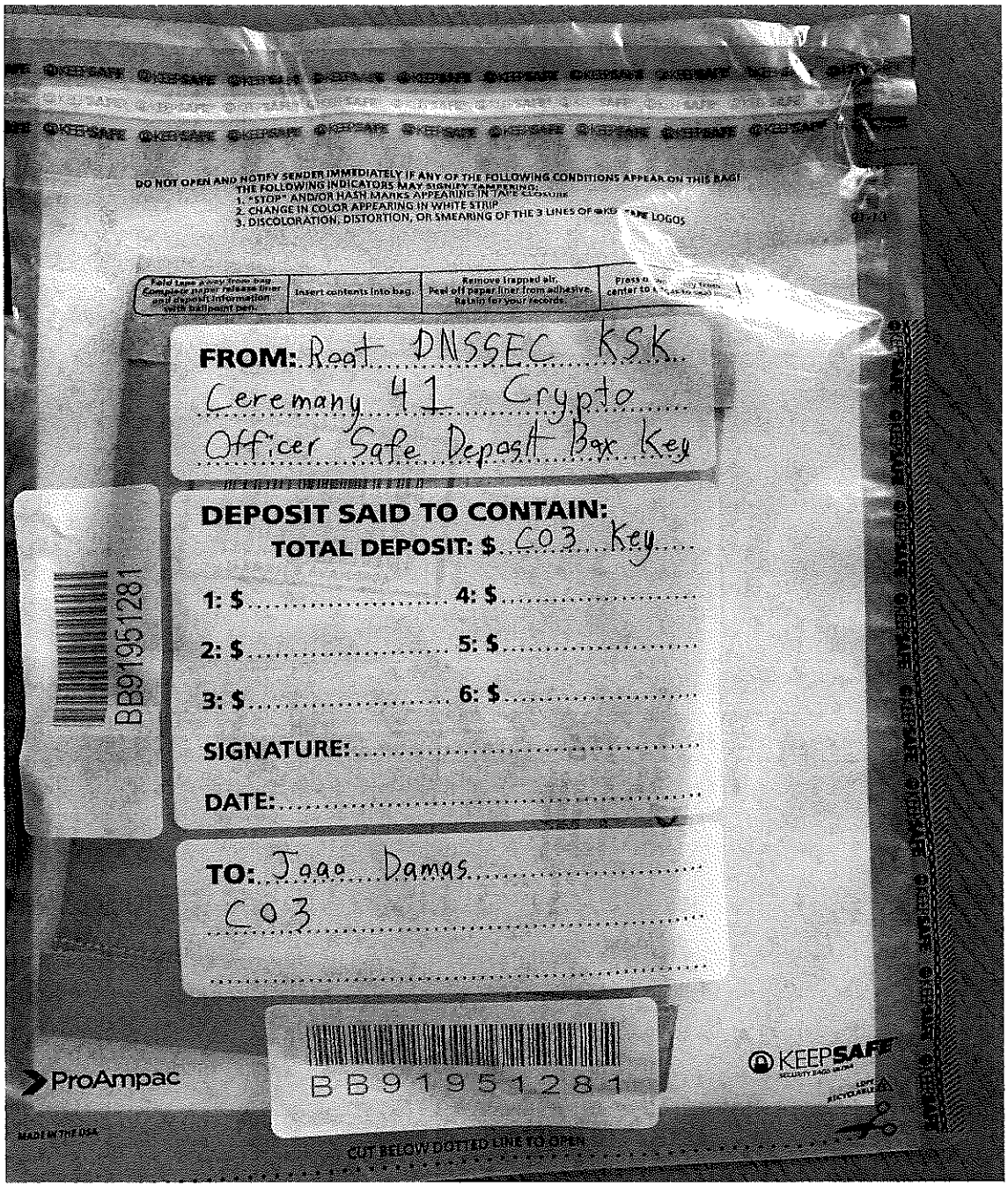
The following photo contains the **CO6 Nicolas Antoniello** Safe Deposit Box **Key TEB # BB91951289** dispatched from the CO.



Appendix I: CO3 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO3 Joao Damas** Safe Deposit Box **Key TEB # BB91951281** dispatched from the CO.

This key has been designated as a backup. The TEB will remain sealed in the courier envelope unless the situation dictates its use. It will be sent back to the CO after the ceremony in its sealed state post-ceremony.



```
ptudor@srx> show configuration
## 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 "XXXXXXXX"; ## SECRET-DATA
    }
    name-server {
        192.0.42.53;
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";

            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA

            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
```

```
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## SECRET-DATA
            }
        }
        user sfreeark {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXX"; ## 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;
    }
}

ptudor@srx>
```