

Root DNSSEC KSK Ceremony 42

Thursday 11 February 2021

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

This ceremony is executed in accordance with the DNSSEC Practice Statement for the Root Zone KSK Operator 6th Edition (2020-11-04)


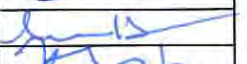
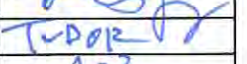


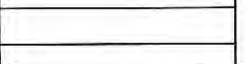
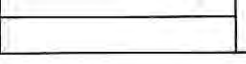
Abbreviations

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

Participants

Key Ceremony roles are described on <https://www.iana.org/help/key-ceremony-roles>

Instructions: At the end of the ceremony, participants sign IW's script. IW records time of completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		2021 Feb 11	20:46
IW	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Hilary Jin / ICANN			
SA	Patrick Tudor / ICANN			
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.	YG	18:00
2	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2.	YG.	18:01
3	CA asks that any first time ceremony participants in the room introduce themselves.	YG.	18:01
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) CO5: Olafur Gudmundsson (Key scripted for use) CO6: Nicolas Antonello (Key scripted for use) CO3: Joao Damas (Key designated as backup) RZM: Duane Wessels / Verisign RZM: Trevor Davis / Verisign AUD: Elvin Paik / RSM	YG.	18:02

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
5	CA reviews emergency evacuation procedures with onsite participants.	YG	18:03
6	CA explains the use of personal electronic devices during the ceremony.	YG	18:03
7	CA summarizes the purpose of the ceremony.	YG	18:04

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: <u>2021-02-11 18:04</u> Note: All entries into this script or any logs should follow this common source of time.	YG.	18:04

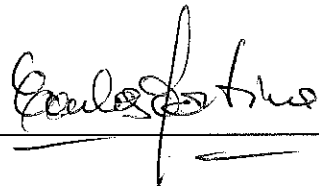
Crypto Officer Safe Deposit Box Key Declaration

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 # BB91951329 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 safe deposit box key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the safe deposit box 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.

TEB # BB91951329

Printed Name CARLOS M. MARTINEZ

Signature 

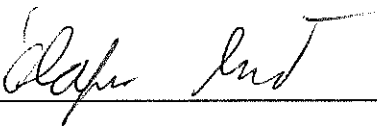
Date 1/15/2021

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 919 51327 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 safe deposit box key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the safe deposit box 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 OLAFUR GUDMUNDSSON

Signature 

Date 2020/01/20

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 Antonello, am hereby entrusting my safe deposit box key enclosed in TEB # BB91951323 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 safe deposit box key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the safe deposit box 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 _____

Nicolas Antonello

Signature _____



Date _____

19 / JAN / 2021

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 # BB91951330 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 safe deposit box key is removed from its TEB and used to operate the safe deposit box lock. I agree to remotely monitor the use of the safe deposit box 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 JOAO LUIS SILVA DAMAS

Signature JLSD

Date 20/ JAN/ 2021

Crypto Officer Key Verification

Step	Activity	Initials	Time
9	<p>The CA performs the following steps to verify the listed CO keys:</p> <ol style="list-style-type: none"> Remove the TEB from the shipping envelope and discard the shipping envelope. Inspect the TEB for tamper evidence. Read aloud the TEB number and place the TEB on the ceremony table visible to the audit camera. Open the TEB and place its contents on the ceremony table. Give the CO key declaration to IW to verify the CO key TEB number then insert the declaration into the audit bundle. Discard the TEB. Remove the CO tenant key from the padded envelope, and set the envelope aside for return shipping post-ceremony. Give the CO tenant key to the IW. <p>CO4: Carlos Martinez Key TEB # BB91951329 (See Appendix F on page 35) ✓</p> <p>CO5: Olafur Gudmundsson Key TEB # BB91951327 (See Appendix G on page 36) ✓</p> <p>CO6: Nicolas Antonello Key TEB # BB91951323 (See Appendix H on page 37) ✓</p> <p>Note 1: The CO3 Joao Damas Safe Deposit Box Key TEB # BB91951330 has been designated as a backup. See Appendix I on page 38.</p> <p>Note 2: The COs' tenant keys were individually transmitted to separate trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.</p>	YG	18:13

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.)	YG	18:14
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 at the first number in the combination.	YG	18:17
12	<p>Perform the following steps to complete the safe log:</p> <ol style="list-style-type: none"> SSC2 removes the existing safe log, then shows the most recent page to the audit camera. IW provides the pre-printed safe log to SSC2. SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies the entry then initials it. 	YG	18:19

Extract CO Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
13	<p>IW performs the following steps sequentially to retrieve the required TEBs:</p> <ul style="list-style-type: none"> a) IW announces the name of the CO whose credentials will be extracted and requests their authorization to open their assigned safe deposit box. b) After the CO provides authorization, 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 opens their assigned 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. <p>CO4: Carlos Martinez Box # 1068 OP TEB # BB91951363 (Retain) SO TEB # BB46584665 (Check and Return)</p> <p>CO5: Olafur Gudmundsson Box # 1789 OP TEB # BB91951362 (Retain) SO TEB # BB46584381 (Check and Return)</p> <p>CO6: Nicolas Antonello Box # 1073 OP TEB # BB91951361 (Retain) SO TEB # BB46584383 (Check and Return)</p>	YG.	18:29

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.	YG.	18:30
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.	YG.	18:31
16	CA, IW, and SSC2 leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	YG.	18:31
17	IW places the TEBs on the ceremony table.	YG.	18:31

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.)	YQ.	18:32
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 at the first number in the combination.	YQ.	18:34
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.	YQ.	18:35

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

Step	Activity	Initials	Time
21	<p>CA performs the following steps to extract each piece of equipment from the safe:</p> <ul style="list-style-type: none"> 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. <p>HSM3: TEB # BB51184234 (Check and Return) ✓ <i>Last Verified: KSK Ceremony 40-AC 2020-02-16</i></p> <p>HSM4: TEB # BB51184238 (Place on Cart) ✓ <i>Last Verified: KSK Ceremony 40 2020-02-16</i></p> <p>HSM5W: TEB # BB51184239 (Check and Return) ✓ <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>Laptop3: TEB # BB81420121 (Check and Return) ✓ <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>Laptop4: TEB # BB81420119 (Place on Cart) ✓ <i>Last Verified: KSK Ceremony 40 2020-02-16</i></p> <p>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384 (Place on Cart) ✓ <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>KSK-2017: TEB # BB46584387 (Check and Return) ✓ <i>Last Verified: KSK Ceremony 38 2019-08-14</i></p> <p>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.</p>	YQ.	18:42

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.	YG.	18:43
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.	YG.	18:43
24	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	YG.	18:44

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
- Synchronize 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	<p>CA performs the following steps to prepare the listed equipment:</p> <ol style="list-style-type: none"> Remove all equipment TEBs from the cart and place them on the ceremony table. Inspect each equipment TEB for tamper evidence. 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. Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. <p>HSM4: TEB # BB51184238 / Serial # H1411006 ✓ <i>Last Verified: KSK Ceremony 40 2020-02-16</i> Laptop4: TEB # BB81420119 / Service Tag # F8SVSG2 ✓ <i>Last Verified: KSK Ceremony 40 2020-02-16</i> OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384 ✓ <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p><i>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.</i></p>	YG.	18:50
2	<p>CA performs the following steps to confirm that no hard drive and battery are in the laptop:</p> <ol style="list-style-type: none"> Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. Open the latch on the left side of the laptop to confirm that the battery slot is empty. 	YG.	18:51
3	<p>CA performs the following steps to boot the laptop:</p> <ol style="list-style-type: none"> Connect the USB printer cable into the rear USB port of the laptop. Connect the null modem cable into the serial port of the laptop. Connect the external HDMI display cable. Connect the power supply. Immediately insert the OS DVD release coen-0.4.0 after the laptop power is switched ON. 	YG.	18:53
4	<p>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</p>	YG.	18:55

OS DVD Checksum Verification

Step	Activity	Initials	Time
5	<p>CA uses the terminal window to executes the following steps:</p> <p>a) Calculate the SHA-256 hash by executing: <code>sha2wordlist < /dev/sr0</code></p> <p>b) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.</p> <p>Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.</p> <p>SHA-256 hash: 8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f</p> <p>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</p> <p>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/42</p>	YG.	18:58

Printer Setup

Step	Activity	Initials	Time
6	<p>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: <code>configure-printer</code></p>	YG.	18:59

Date Setup

Step	Activity	Initials	Time
7	<p>CA executes <code>date</code> using the terminal window to verify if the date/time reasonably matches the ceremony clock.</p> <p>If the date/time do not match, perform the following steps:</p> <p>a) Execute <code>date -s "20210211 HH:MM:00"</code> to set the time. where <code>HH</code> is two-digit hour, <code>MM</code> is two-digit minutes and <code>00</code> is zero seconds.</p> <p>b) Execute <code>date</code> to confirm the date/time matches the clock.</p>	YG.	19:00

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the Ceremony 41 HSMFD into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window.	YG	19:01
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: <code>hsmfd-hash -c</code> 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 2020/04/23 <code># find -P /media/HSMFD/ -type f -print0 sort -z xargs -0 cat sha2wordlist</code> 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 IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 41 annotated script.	YG	19:03

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused HSMFD 41 and the sheet of paper with the printed HSMFD hash to RKOS.	YG	19:03

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: <code>cd /media/HSMFD</code>	YG	19:04
12	CA executes the command below to log activities of the Commands terminal window: <code>script script-20210211.log</code>	YG	19:04

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: <code>cd /media/HSMFD</code> b) Set the serial port baud rate by executing: <code>stty -F /dev/ttyS0 115200</code> c) Start logging the serial output by executing: <code>ttyaudit /dev/ttyS0</code> Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.	YG	19:06

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none">a) Verify the label on the HSM reads HSM4b) 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. <p>Note: Status information should appear on the HSM activity logging screen.</p> <ul style="list-style-type: none">e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads H1411006, then scroll back to the bottom. <p>HSM4: Serial # H1411006 ✓</p> <p>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</p>	YG.	19:08

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

Using the krsigner 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 krsigner application uses the private key stored in the HSM to generate the SKR containing the digital signatures of the ZSK slated for future use
- 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	<p>CA performs the following steps to verify the COs' credentials:</p> <p>a) Read aloud the TEB number, then inspect it for tamper evidence.</p> <p>b) Open the TEB, then remove the plastic case containing the card(s).</p> <p>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.</p> <p>CO4: Carlos Martinez OP TEB # BB91951363 ✓</p> <p>CO5: Olafur Gudmundsson OP TEB # BB91951362 ✓</p> <p>CO6: Nicolas Antonello OP TEB # BB91951361 ✓</p>	YGT.	19-12

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
2	<p>CA performs the following steps to activate the HSM:</p> <p>a) Utilize the HSM's keyboard to scroll through the menu using <></p> <p>b) Select "1.Set Online", press ENT to confirm.</p> <p>c) When "Set Online?" is displayed, press ENT to confirm.</p> <p>d) When "Insert Card OP #X?" is displayed, insert the OP card.</p> <p>e) When "PIN?" is displayed, enter "11223344", then press ENT.</p> <p>f) When "Remove Card?" is displayed, remove the OP card.</p> <p>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.</p> <p>Confirm the "READY" LED on the HSM is ON.</p> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>1st OP card <u>4</u> of 7</p> <p>2nd OP card <u>5</u> of 7</p> <p>3rd OP card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	YGT.	19-15

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.	YH.	19:16
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: <code>ping hsm</code> c) Wait for responses, then exit by pressing: <code>Ctrl + C</code>	YH.	19:16

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. The first for the next calendar quarter and the remainder for subsequent quarter(s).	YH.	19:18

Execute the KSR Signer for KSR 2021 Q2

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: <code>ksrsigner /media/KSR/KSK42-2021-Q2/ksr-root-2021-q2-0.xml</code>	YH.	19:19
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.	YH.	19:19



February 11, 2021

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

To Whom It May Concern:

Verisign.com

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 – Product Operations 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 23 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 163.7 million .com and .net domain names and processing more than 219 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,

2/10/2021

X 

Dave Carney
HR Specialist
Signed by: Carney, David

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



VERISIGN™

11 February 2021

The SHA256 hash of the 2021 Q2 KSR file is:

ksr-root-2021-q2-0.xml:

504950019bfc676d0aacf720845b1912c2f5c4dc0f3292f8868d9e4651d568eb

The PGP wordlist for the hash above is:

PGP Words: drumbeat dinosaur drumbeat adviser puppy Wilmington
freedom hazardous allow penetrate virus butterfat mural exodus bedlamp
backwater snapshot visitor snowslide sympathy artist component physique
warranty necklace microscope quiver detergent drunken specialist frighten
underfoot

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



VERISIGN™

11 February 2021

The SHA256 hash of the 2021 Q3 KSR file is:

ksr-root-2021-q3-0.xml:

68c413bf5ecd4e5867cc0a21c0a5508b74d150ba2096ee0d623df714ac93f5bb

The PGP wordlist for the hash above is:

PGP words: frighten reproduce Aztec rebellion eyeglass sandalwood drifter
everyday freedom revolver allow Camelot slowdown paperweight drumbeat
Medusa indoors scavenger drumbeat puberty bison monument tycoon
asteroid flagpole crucifix virus belowground ribcage molasses vapor publisher

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



VERISIGN™

11 February 2021

The SHA256 hash of the 2021 Q4 KSR file is:

ksr-root-2021-q4-0.xml:

7a545e81f5332e99112fb8f68154d8c111f8e9074c5840cd8062cad8c0e06906

The PGP wordlist for the hash above is:

PGP words: keyboard equation eyeglass inventive vapor concurrent buzzard
nebula Athens combustion select vocalist minnow equation stormy recover
Athens warranty treadmill amusement drainage everyday crackdown
sandalwood merit gadgetry spellbind stupendous slowdown tobacco gazelle
amulet

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

Verify the KSR Hash for KSR 2021 Q2

Step	Activity	Initials	Time
8	<p>When the hash of the KSR is displayed in the terminal window, perform the following:</p> <p>a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification off camera for the purpose of authentication while maintaining privacy.</p> <p>Note: If the RZM representative is not physically present in the room, write the representative's name and "<i>Remote Participant</i>" next to the name on the signature line.</p> <p>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:</p> <p>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.</p> <p>^{y.y.} DA <u>TREVOR LEWIS DAVIS</u></p> <p>c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.</p>	Y.G.	19:22
9	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks " are there any objections? "	Y.G.	19:22
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/KSK42-2021-Q2/skr-root-2021-q2-0.xml	Y.G.	19:23

Execute the KSR Signer for KSR 2021 Q3

Step	Activity	Initials	Time
11	CA executes the command below in the terminal window to copy the previous quarter's generated SKR to construct a chain of trust to the subsequent KSR: cp /media/KSR/KSK42-2021-Q2/skr-root-2021-q2-0.xml /media/KSR/KSK42-2021-Q3/skr.xml	Y.G.	19:24
12	<p>CA executes the command below in the terminal window to sign the KSR file: ksrsigner /media/KSR/KSK42-2021-Q3/ksr-root-2021-q3-0.xml</p> <p>Note: It is anticipated that the KSR Signer Software will issue a warning if one or more of the request's signatures will exceed the limit of 180 days of expiration in the future. All SKRs will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set will not expire more than 180 days in the future.</p>	Y.G.	19:26
13	<p>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.</p>	Y.G.	19:26

Verify the KSR Hash for KSR 2021 Q3

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.	YG.	19:27
15	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks "are there any objections?"	YG.	19:27
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/KSK42-2021-Q3/skr-root-2021-q3-0.xml	YG.	19:28

Execute the KSR Signer for KSR 2021 Q4

Step	Activity	Initials	Time
17	CA executes the command below in the terminal window to copy the previous quarter's generated SKR to construct a chain of trust to the subsequent KSR: cp /media/KSR/KSK42-2021-Q3/skr-root-2021-q3-0.xml /media/KSR/KSK42-2021-Q4/skr.xml	YG.	19:29
18	CA executes the command below in the terminal window to sign the KSR file: ksrsigner /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml Note: It is anticipated that the KSR Signer Software will issue a warning if one or more of the request's signatures will exceed the limit of 180 days of expiration in the future. All SKRs will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set will not expire more than 180 days in the future.	YG.	19:30
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.	YG.	19:30

Verify the KSR Hash for KSR 2021 Q4

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.	YG.	19:31
21	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks "are there any objections?"	YG.	19:31
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/KSK42-2021-Q4/skr-root-2021-q4-0.xml	YG.	19:31

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-202102*.log); do printlog \$i; done	YG.	19:34
24	IW attaches a copy of the required ksrsigner log to their script.	YG.	19:35

Starting: ksrsigner /media/KSR/KSK42-2021-Q2/ksr-root-2021-q2-0.xml (at Thu Feb 11 19:18:56 2021 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
RSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:

Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1411006

Validating last SKR with HSM...

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR validation data.

Validate and Process KSR /media/KSR/KSK42-2021-Q2/ksr-root-2021-q2-0.xml...

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR processing data.

SHA256 hash of KSR:

504950019BFC676D0AACF720845B1912C2F5C4DC0F3292F8868D9E4651D568EB

>> drumbeat dinosaur drumbeat adviser puppy Wilmington freedom hazardous allow penetrate virus butterfat mural exodus bed lamp backwater snapshot visitor snowslide sympathy artist component physique warranty necklace microscope quiver detergent drunken specialist frighten underfoot <<

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/KSK42-2021-Q2/skr-root-2021-q2-0.xml

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of new SKR generation data.

SHA256 hash of SKR:

495669C6407D11D5E2F2D0D3F96D2D606E03F941A5CD80D9A7CC20F98C1C8B9A

>> deckhand escapade gazelle responsive crackdown insincere Athens specialist tiger vagabond stagnate sociable waffle haz arduous button fortitude goldfish aggregate waffle decadence reindeer sandalwood merit supportive repay revolver bison Waterloo offload Brazilian obtuse newsletter <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0

Starting: ksrsigner /media/KSR/KSK42-2021-Q3/ksr-root-2021-q3-0.xml (at Thu Feb 11 19:25:46 2021 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: ICANNRKS
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1411006

Validating last SKR with HSM...

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR validation data.

Validate and Process KSR /media/KSR/KSK42-2021-Q3/ksr-root-2021-q3-0.xml...

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR processing data and signature expiration warnings.

SHA256 hash of KSR:
68C413BF5ECD4E5867CC0A21C0A5508B74D150BA2096EE0D623DF714AC93F5BB

>> frighten reproduce Aztec rebellion eyeglass sandalwood drifter everyday freedom revolver allow Camelot slowdown paperw
eight drumbeat Medusa indoors scavenger drumbeat puberty bison monument tycoon asteroid flagpole crucifix virus belowgrou
nd ribcage molasses vapor publisher <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"

Table with 1 column: # KSK Tag(CKA_LABEL). Contains 9 rows of KSK tags.

Generated new SKR in /media/KSR/KSK42-2021-Q3/skr-root-2021-q3-0.xml

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of new SKR generation data.

SHA256 hash of SKR:
0CC8563AAA6FBEF52804D2957FAA48E2576FF83F2A40CCF201E69022AA1BE28C

>> ammo retrieval egthead corrosion reward hemisphere skydive visitor breadline alkali standard Montana lockup pedigree d
eadbolt tomorrow eightball hemisphere Vulcan customer brickyard Dakota spigot vagabond absurd trombonist peachy candidate
reward bravado tiger megaton <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0

Starting: ksrsigner /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml (at Thu Feb 11 19:29:52 2021 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:

Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1411006

Validating last SKR with HSM...

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR data.

Validate and Process KSR /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml...

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR data and 8 lines of signature expiration warnings.

SHA256 hash of KSR:

7A545E81F5332E99112FB8F68154D8C111F8E9074C5840CD8062CAD8C0E0690F

>> keyboard equation eyeglass inventive vapor concurrent buzzard nebula Athens combustion select vocalist minnow equation
stormy recover Athens warranty treadmill amusement drainage everyday crackdown sandalwood merit gadgetry spellbind stupe
ndous slowdown tobacco gazelle amulet <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"

Table with 1 column: KSK Tag(CKA_LABEL). Contains 9 rows of KSK tags.

Generated new SKR in /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml

Table with 4 columns: #, Inception, Expiration, ZSK Tags, KSK Tag(CKA_LABEL). Contains 9 rows of SKR data.

SHA256 hash of SKR:

00AF72E5321B72CDCE6EBF9B23CD6AA6C89450EE429D85ACCAFBE1E2A47485BF

>> aardvark pharmacy highchair travesty checkup bravado highchair sandalwood spyglass headwaters slingshot Norwegian blow
torch sandalwood Geiger paragon spaniel molecule drumbeat universe crowfoot Ohio music penetrate spellbind Wichita berser
k Capricorn regain hydraulic music rebellion <<

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	<p>CA executes the following commands using the terminal window:</p> <p>a) List the contents of the KSRFD by executing: <code>ls -ltrR /media/KSR</code></p> <p>b) Copy the contents of the KSRFD to the HSMFD by executing: <code>cp -pR /media/KSR/* .</code></p> <p>Note: Confirm overwrite by entering "y" if prompted.</p> <p>c) List the contents of the HSMFD to verify it has been copied successfully by executing: <code>ls -ltrR</code></p> <p>d) Unmount the KSRFD by executing: <code>umount /media/KSR</code></p>	YG.	19:37
26	CA removes the KSRFD containing the SKR files, then gives it to RKOS.	YG.	19:37

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
27	<p>CA deactivates the HSM by performing the following steps:</p> <p>Note: CA will use OP cards not previously utilized in this ceremony if available.</p> <p>a) CA displays the HSM activity logging terminal window</p> <p>b) Utilize the HSM's keyboard to scroll through the menu using < ></p> <p>c) Select "2.Set Offline", press ENT to confirm.</p> <p>d) When "Set Offline?" is displayed, press ENT to confirm.</p> <p>e) When "Insert Card OP #X?" is displayed, insert the OP card from the card holder.</p> <p>f) When "PIN?" is displayed, enter "11223344", then press ENT.</p> <p>g) When "Remove Card?" is displayed, remove the OP card.</p> <p>h) Repeat steps e) to g) for the 2nd and 3rd OP cards.</p> <p>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.</p> <p>1st OP card <u>4</u> of 7 2nd OP card <u>6</u> of 7 3rd OP card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	YG.	19:40

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.	YG.	19:41
29	CA places the HSM into a prepared TEB, then seals it.	YG.	19:42
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. HSM4: TEB # BB51184285 / Serial # H1411006 ✓	YG.	19:43

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.	YOT.	19:45

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

SHA-256: 4789eb79389bcf988cda934ba60c07b694664e60343bed937b41b739908f46bd

PGP Words: dashboard matchmaker trouble inertia classic Norwegian stagehand narrative offload surrender playhouse disable rematch article ahead potato Pluto gossamer drifter fortitude choking councilman tunnel molasses kickoff decadence seabird corporate peachy midsummer cubic quantity

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: <code>shopt -s dotglob</code>	YGT	19:46
3	CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content: a) <code>lpadmin -p HP -o copies-default=2</code> b) <code>hsmfd-hash -p</code> Note: One copy for audit bundle and one copy for HSMFD package.	YGT	19:47
4	CA executes the command below using the terminal window to display the contents of the HSMFD: <code>ls -ltrR</code>	YGT	19:47
5	CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs: <code>mkdir /media/HSMFD1</code>	YGT	19:47
6	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.	YGT	19:48
7	CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: <code>df</code>	YGT	19:49
8	CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD: a) <code>umount /dev/sdc1</code> b) <code>mkfs.vfat -n HSMFD -I /dev/sdc1</code> c) <code>mount /dev/sdc1 /media/HSMFD1</code> d) <code>cp -pR * /media/HSMFD1</code>	YGT	19:50
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) <code>hsmfd-hash -m</code> b) <code>umount /media/HSMFD1</code>	YGT	19:51
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.	YGT	19:51
11	CA repeats step 6 to 10 for the 2 nd copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	YGT	19:53
12	CA repeats step 6 to 10 for the 3 rd copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	YGT	19:55
13	CA repeats step 6 to 10 for the 4 th copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	YGT	19:56
14	CA repeats step 6 to 10 for the 5 th copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	YGT	19:58

02/11/21
19:45:27

script-20210211.log

1

```
Script started on Thu Feb 11 19:04:56 2021
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=0.830 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.574 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.746 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.567 ms
64 bytes from hsm (192.168.0.2): icmp_seq=5 ttl=255 time=0.558 ms
64 bytes from hsm (192.168.0.2): icmp_seq=6 ttl=255 time=0.569 ms
64 bytes from hsm (192.168.0.2): icmp_seq=7 ttl=255 time=0.562 ms
^C
--- hsm ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6126ms
rtt min/avg/max/mdev = 0.558/0.629/0.830/0.105 ms
root@coen:/media/HSMFD# ksrsgner /media/KSR/KSK\00742-2021-Q2\k007sr-root-2021-q2-0.xml
```

```
Starting: ksrsgner /media/KSR/KSK42-2021-Q2/ksr-root-2021-q2-0.xml (at Thu Feb 11 19:18:56 2021 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_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
```

```
Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1411006
```

```
Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 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
...VALIDATED.
```

```
Validate and Process KSR /media/KSR/KSK42-2021-Q2/ksr-root-2021-q2-0.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-04-01T00:00:00 2021-04-22T00:00:00 14631,42351
2 2021-04-11T00:00:00 2021-05-02T00:00:00 14631
3 2021-04-21T00:00:00 2021-05-12T00:00:00 14631
4 2021-05-01T00:00:00 2021-05-22T00:00:00 14631
5 2021-05-11T00:00:00 2021-06-01T00:00:00 14631
6 2021-05-21T00:00:00 2021-06-11T00:00:00 14631
7 2021-05-31T00:00:00 2021-06-21T00:00:00 14631
8 2021-06-10T00:00:00 2021-07-01T00:00:00 14631
9 2021-06-20T00:00:00 2021-07-11T00:00:00 14631,26838
...PASSED.
```

```
SHA256 hash of KSR:
504950019BFC676D0AACF720845B1912C2F5C4DC0F3292F8868D9E4651D568EB
>> drumbeat dinosaur drumbeat adviser puppy Wilmington freedom hazardous allow penetrate
```

```
virus butterfat mural exodus bedlamp backwater snapshot visitor snowslide sympathy artist
component physique warranty necklace microscope quiver detergent drunken specialist frig
hten underfoot <<
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/KSK42-2021-Q2/skr-root-2021-q2-0.xml
```

```
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-04-01T00:00:00 2021-04-22T00:00:00 42351,14631 20326(Klajeyz)/S
2 2021-04-11T00:00:00 2021-05-02T00:00:00 14631 20326(Klajeyz)/S
3 2021-04-21T00:00:00 2021-05-12T00:00:00 14631 20326(Klajeyz)/S
4 2021-05-01T00:00:00 2021-05-22T00:00:00 14631 20326(Klajeyz)/S
5 2021-05-11T00:00:00 2021-06-01T00:00:00 14631 20326(Klajeyz)/S
6 2021-05-21T00:00:00 2021-06-11T00:00:00 14631 20326(Klajeyz)/S
7 2021-05-31T00:00:00 2021-06-21T00:00:00 14631 20326(Klajeyz)/S
8 2021-06-10T00:00:00 2021-07-01T00:00:00 14631 20326(Klajeyz)/S
9 2021-06-20T00:00:00 2021-07-11T00:00:00 26838,14631 20326(Klajeyz)/S
```

```
SHA256 hash of SKR:
495669C6407D11D5E2F2D0D3F96D2D60E03F941A5CD80D9A7CC20F98C1C8B9A
>> deckhand escapade gazelle responsive crackdown insincere Athens specialist tiger vagabond
stagnate sociable waffle hazardous button fortitude goldfish aggregate waffle decadence
reindeer sandalwood merit supportive repay revolver bison Waterloo offload Brazilian obtuse
newsletter <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

```
***** Log output in ./ksrsgner-20210211-191856.log *****
root@coen:/media/HSMFD# cp /media/KSR/KSK\00742-2021-Q2/skr\007-root-2021-q2-0.xml /media/KSR/KSK\00742-2021-Q3/s
root@coen:/media/HSMFD# ksrsgner /media/KSR/KSK\00742-2021-Q3/k\007sr-root-2021-q3-0.xml
```

```
Starting: ksrsgner /media/KSR/KSK42-2021-Q3/ksr-root-2021-q3-0.xml (at Thu Feb 11 19:25:46 2021 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_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1411006
```

```
Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-04-01T00:00:00 2021-04-22T00:00:00 42351,14631 20326(Klajeyz)/S
```

02/11/21
19:45:27

script-20210211.log

2

```
2 2021-04-11T00:00:00 2021-05-02T00:00:00 14631 20326(Klajeyz)/S
3 2021-04-21T00:00:00 2021-05-12T00:00:00 14631 20326(Klajeyz)/S
4 2021-05-01T00:00:00 2021-05-22T00:00:00 14631 20326(Klajeyz)/S
5 2021-05-11T00:00:00 2021-06-01T00:00:00 14631 20326(Klajeyz)/S
6 2021-05-21T00:00:00 2021-06-11T00:00:00 14631 20326(Klajeyz)/S
7 2021-05-31T00:00:00 2021-06-21T00:00:00 14631 20326(Klajeyz)/S
8 2021-06-10T00:00:00 2021-07-01T00:00:00 14631 20326(Klajeyz)/S
9 2021-06-20T00:00:00 2021-07-11T00:00:00 26838,14631 20326(Klajeyz)/S
...VALIDATED.
```

Validate and Process KSR /media/KSR/KSK42-2021-Q3/ksr-root-2021-q3-0.xml...

```
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-07-01T00:00:00 2021-07-22T00:00:00 14631,26838
2 2021-07-11T00:00:00 2021-08-01T00:00:00 26838
3 2021-07-21T00:00:00 2021-08-11T00:00:00 26838
4 2021-07-31T00:00:00 2021-08-21T00:00:00 26838
5 2021-08-10T00:00:00 2021-08-31T00:00:00 26838
6 2021-08-20T00:00:00 2021-09-10T00:00:00 26838
7 2021-08-30T00:00:00 2021-09-20T00:00:00 26838
8 2021-09-09T00:00:00 2021-09-30T00:00:00 26838
9 2021-09-19T00:00:00 2021-10-10T00:00:00 14748,26838
[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:

68C413BF5ECC4E5867CC0A21C0A5508B74D150BA2096EED0623DF714AC93F5BB

>> frighten reproduce Aztec rebellion eyeglass sandalwood drifter everyday freedom revolve
er allow Camelot slowdown paperweight drumbeat Medusa indoors scavenger drumbeat puberty
bison monument tycoon asteroid flagpole crucifix virus belowground ribcage molasses vapor
publisher <<
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/KSK42-2021-Q3/skr-root-2021-q3-0.xml

```
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-07-01T00:00:00 2021-07-22T00:00:00 26838,14631 20326(Klajeyz)/S
2 2021-07-11T00:00:00 2021-08-01T00:00:00 26838 20326(Klajeyz)/S
3 2021-07-21T00:00:00 2021-08-11T00:00:00 26838 20326(Klajeyz)/S
4 2021-07-31T00:00:00 2021-08-21T00:00:00 26838 20326(Klajeyz)/S
5 2021-08-10T00:00:00 2021-08-31T00:00:00 26838 20326(Klajeyz)/S
6 2021-08-20T00:00:00 2021-09-10T00:00:00 26838 20326(Klajeyz)/S
7 2021-08-30T00:00:00 2021-09-20T00:00:00 26838 20326(Klajeyz)/S
8 2021-09-09T00:00:00 2021-09-30T00:00:00 26838 20326(Klajeyz)/S
9 2021-09-19T00:00:00 2021-10-10T00:00:00 26838,14748 20326(Klajeyz)/S
```

SHA256 hash of SKR:

0CC8563AAA6FBEF52804D2957FAA48E2576FF83F2A40CCF201E69022AA1BE28C

>> ammo retrieval egghead corrosion reward hemisphere skydive visitor breadline alkali st

andard Montana lockup pedigree deadbolt tomorrow eightball hemisphere Vulcan customer bri
ckyard Dakota spigot vagabond absurd trombonist peachy candidate reward bravado tiger meg
aton <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

***** Log output in ./ksrsigner-20210211-192546.log *****

root@coen:/media/HSMFD# cp /media/KSR/KS\007K42-2021-Q3/skr\007-root-2021-q3-0.xml /media
KSR/KS\007SK42-2021-Q4/s

root@coen:/media/HSMFD# ksrsigner /media/KSR/KS\007K42-2021-Q4/ksr-root-2021-q4-0.xml
Starting: ksrsigner /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml (at Thu Feb 11 19:29:
52 2021 UTC)

Use HSM /opt/dnssec/aep.hsmconfig?

Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.

[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec

[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glib
c_2_5_x86_64.so.5.02

Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.s
o.5.02

HSM slot 0 included

Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0

HSM information:

```
Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1411006
```

Validating last SKR with HSM...

```
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-07-01T00:00:00 2021-07-22T00:00:00 26838,14631 20326(Klajeyz)/S
2 2021-07-11T00:00:00 2021-08-01T00:00:00 26838 20326(Klajeyz)/S
3 2021-07-21T00:00:00 2021-08-11T00:00:00 26838 20326(Klajeyz)/S
4 2021-07-31T00:00:00 2021-08-21T00:00:00 26838 20326(Klajeyz)/S
5 2021-08-10T00:00:00 2021-08-31T00:00:00 26838 20326(Klajeyz)/S
6 2021-08-20T00:00:00 2021-09-10T00:00:00 26838 20326(Klajeyz)/S
7 2021-08-30T00:00:00 2021-09-20T00:00:00 26838 20326(Klajeyz)/S
8 2021-09-09T00:00:00 2021-09-30T00:00:00 26838 20326(Klajeyz)/S
9 2021-09-19T00:00:00 2021-10-10T00:00:00 26838,14748 20326(Klajeyz)/S
...VALIDATED.
```

Validate and Process KSR /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml...

```
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-10-01T00:00:00 2021-10-22T00:00:00 14748,26838
2 2021-10-11T00:00:00 2021-11-01T00:00:00 14748
3 2021-10-21T00:00:00 2021-11-11T00:00:00 14748
4 2021-10-31T00:00:00 2021-11-21T00:00:00 14748
5 2021-11-10T00:00:00 2021-12-01T00:00:00 14748
6 2021-11-20T00:00:00 2021-12-11T00:00:00 14748
7 2021-11-30T00:00:00 2021-12-21T00:00:00 14748
8 2021-12-10T00:00:00 2021-12-31T00:00:00 14748
9 2021-12-20T00:00:00 2022-01-10T00:00:00 09799,14748
```

[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.

02/11/21
19:45:27

script-20210211.log

3

```
SHA256 hash of KSR:
7A545E81F5332E99112FB8F68154D8C111F8E9074C5840CD8062CAD8C0E06906
>> keyboard equation eyeglass inventive vapor concurrent buzzard nebula Athens combustion
select vocalist minnow equation stormy recover Athens warranty treadmill amusement drain
age everyday crackdown sandalwood merit gadgetry spellbind stupendous slowdown tobacco ga
zelle amulet <<
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/KSK42-2021-Q4/skr-root-2021-q4-0.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2021-10-01T00:00:00 2021-10-22T00:00:00 26838,14748 20326(Klajeyz)/S
2 2021-10-11T00:00:00 2021-11-01T00:00:00 14748 20326(Klajeyz)/S
3 2021-10-21T00:00:00 2021-11-11T00:00:00 14748 20326(Klajeyz)/S
4 2021-10-31T00:00:00 2021-11-21T00:00:00 14748 20326(Klajeyz)/S
5 2021-11-10T00:00:00 2021-12-01T00:00:00 14748 20326(Klajeyz)/S
6 2021-11-20T00:00:00 2021-12-11T00:00:00 14748 20326(Klajeyz)/S
7 2021-11-30T00:00:00 2021-12-21T00:00:00 14748 20326(Klajeyz)/S
8 2021-12-10T00:00:00 2021-12-31T00:00:00 14748 20326(Klajeyz)/S
9 2021-12-20T00:00:00 2022-01-10T00:00:00 09799,14748 20326(Klajeyz)/S
```

```
SHA256 hash of SKR:
00AF72E5321B72CDCE6EBF9B23CD6AA6C89450EE429D85ACCAFBE24A47485BF
>> aardvark pharmacy highchair travesty checkup bravado highchair sandalwood spyglass hea
dwaters slingshot Norwegian blowtorch sandalwood Geiger paragon spaniel molecule drumbeat
universe crowfoot Ohio music penetrate spellbind Wichita berserk Capricorn regain hydrau
lic music rebellion <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0
```

```
***** Log output in ./ksrsigner-20210211-192952.log *****
root@coen:/media/HSMFD# lpadmin -p BP -c copies-default=M
root@coen:/media/HSMFD# for i in $(ls -l ksrsigner-20210211log); 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 Feb 11 19:23 \033[0m\033[01;34mKSK42-2021-Q2\033[0m
drwxr-xr-x 2 root root 16384 Feb 11 19:28 \033[01;34mKSK42-2021-Q3\033[0m
drwxr-xr-x 2 root root 16384 Feb 11 19:31 \033[01;34mKSK42-2021-Q4\033[0m
```

```
/media/KSR/KSK42-2021-Q2:
total 144
-rw-r--r-- 1 root root 20369 Feb 8 22:09 skr.xml.20210211191856
-rw-r--r-- 1 root root 19600 Feb 8 22:09 ksr-root-2021-q2-0.xml
-rw-r--r-- 1 root root 1148 Feb 8 22:09 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11 19:23 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11 19:23 skr-root-2021-q2-0.xml
```

```
/media/KSR/KSK42-2021-Q3:
total 144
-rw-r--r-- 1 root root 19600 Feb 8 22:09 ksr-root-2021-q3-0.xml
-rw-r--r-- 1 root root 1148 Feb 8 22:09 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11 19:24 skr.xml.20210211192546
-rw-r--r-- 1 root root 20369 Feb 11 19:28 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11 19:28 skr-root-2021-q3-0.xml
```

```
/media/KSR/KSK42-2021-Q4:
total 144
-rw-r--r-- 1 root root 19598 Feb 8 22:09 ksr-root-2021-q4-0.xml
-rw-r--r-- 1 root root 1148 Feb 8 22:09 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11 19:29 skr.xml.20210211192952
-rw-r--r-- 1 root root 20369 Feb 11 19:31 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11 19:31 skr-root-2021-q4-0.xml
root@coen:/media/HSMFD# cp -pR /media/KSR/* .
root@coen:/media/HSMFD# ls -ltrR
.:
total 3200
-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
```

script-20210211.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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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
-rw-r--r-- 1 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 2020 ksrsigner-20200216-022133.log
-rw-r--r-- 1 root root 8192 Feb 16 2020 \033[01;34mKSK40\033[0m
-rw-r--r-- 1 root root 12174 Feb 16 2020 ttyaudit-ttyS0-20200216-020929.log
-rw-r--r-- 1 root root 23671 Feb 16 2020 script-20200216.log
-rw-r--r-- 1 root root 6308 Apr 23 2020 ksrsigner-20200423-184208.log
-rw-r--r-- 1 root root 8192 Apr 23 2020 \033[01;34mKSK41-2020-Q3\033[0m
-rw-r--r-- 1 root root 7151 Apr 23 2020 ksrsigner-20200423-185053.log
-rw-r--r-- 1 root root 8192 Apr 23 2020 \033[01;34mKSK41-2020-Q4\033[0m
-rw-r--r-- 1 root root 7151 Apr 23 2020 ksrsigner-20200423-185433.log
-rw-r--r-- 1 root root 8192 Apr 23 2020 \033[01;34mKSK41-2021-Q1\033[0m
-rw-r--r-- 1 root root 15125 Apr 23 2020 ttyaudit-ttyS0-20200423-182706.log
```

02/11/21
19:45:27

script-20210211.log

5

```
-rw-r--r-- 1 root root 36962 Apr 23 2020 script-20200423.log
-rw-r--r-- 1 root root 6295 Feb 11 19:23 ksrsigner-20210211-191856.log
drwxr-xr-x 2 root root 8192 Feb 11 19:23 \033[01;34mKSK42-2021-Q2\033[0m
-rw-r--r-- 1 root root 6958 Feb 11 19:28 ksrsigner-20210211-192546.log
drwxr-xr-x 2 root root 8192 Feb 11 19:28 \033[01;34mKSK42-2021-Q3\033[0m
-rw-r--r-- 1 root root 12858 Feb 11 19:31 ttyaudit-ttyS0-20210211-190608.log
drwxr-xr-x 2 root root 8192 Feb 11 19:31 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root 7169 Feb 11 19:31 ksrsigner-20210211-192952.log
drwxr-xr-x 2 root root 8192 Feb 11 19:31 \033[01;34mKSK42-2021-Q4\033[0m
-rw-r--r-- 1 root root 16384 Feb 11 19:35 script-20210211.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 2020 skr.xml.20200216022133
-rw-r--r-- 1 root root 19600 Feb 4 2020 ksr-root-2020-q2-0.xml
-rw-r--r-- 1 root root 1148 Feb 4 2020 kskschedule.json
```

02/11/21
19:45:27

script-20210211.log

6

```
-rw-r--r-- 1 root root 20369 Feb 16 2020 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16 2020 skr-root-2020-q2-0.xml

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

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

./KSK41-2021-Q1:
total 104
-rw-r--r-- 1 root root 19600 Apr 22 2020 ksr-root-2021-q1-0.xml
-rw-r--r-- 1 root root 1148 Apr 22 2020 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 23 2020 skr.xml.20200423185433
-rw-r--r-- 1 root root 20369 Apr 23 2020 skr.xml
-rw-r--r-- 1 root root 20369 Apr 23 2020 skr-root-2021-q1-0.xml

./KSK42-2021-Q2:
total 104
-rw-r--r-- 1 root root 20369 Feb 8 22:09 skr.xml.20210211191856
-rw-r--r-- 1 root root 19600 Feb 8 22:09 ksr-root-2021-q2-0.xml
-rw-r--r-- 1 root root 1148 Feb 8 22:09 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11 19:23 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11 19:23 skr-root-2021-q2-0.xml

./KSK42-2021-Q3:
total 104
-rw-r--r-- 1 root root 19600 Feb 8 22:09 ksr-root-2021-q3-0.xml
-rw-r--r-- 1 root root 1148 Feb 8 22:09 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11 19:24 skr.xml.20210211192546
-rw-r--r-- 1 root root 20369 Feb 11 19:28 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11 19:28 skr-root-2021-q3-0.xml

./tmp:
total 72
-rw-r--r-- 1 root root 1768 Feb 11 19:31 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.3
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Feb 11 19:31 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Feb 11 19:31 skr.keybundle.0

./KSK42-2021-Q4:
total 104
-rw-r--r-- 1 root root 19598 Feb 8 22:09 ksr-root-2021-q4-0.xml
-rw-r--r-- 1 root root 1148 Feb 8 22:09 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11 19:29 skr.xml.20210211192952
-rw-r--r-- 1 root root 20369 Feb 11 19:31 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11 19:31 skr-root-2021-q4-0.xml
root@coen:/media/HSMFD# umount/media/KSR/
k038@coen:/media/HSMFD# exit
```

exit

Script done on Thu Feb 11 19:45:27 2021

```
2021-02-11T19:07:34+0000 ttyS0 bbbby
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 H1411006 011397 BBL 010 : Factory Software Verification Key : CPLD version 1.9
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 BBL CRC32: 0x757574CA
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 Running applicationBootLoader at 0xEFDC0000
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 H1411006 011403 ABL 011 : Tamper Challenge Response Key
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 ABL CRC32: 0xE7E0FA6A
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 #####
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 ### ABL tamper records ###
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 #####
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 =====
2021-02-11T19:07:34+0000 ttyS0 vextoosTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 vintoosTamperCount: 15
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 vbboosTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 maxstrtempTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 minstrtempTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 meshTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 extampSMKTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 extampIMKTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 tempdiffTamperCount: 0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 pFTamperCount: 15
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 restartTamperCount: 47
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 Current tamper bitmaps:
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 =====
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 currentTamper bitmap: 0x0000 0b ....
2021-02-11T19:07:34+0000 ttyS0
2021-02-11T19:07:34+0000 ttyS0 lastTamper bitmap: 0x0080 0b .... 1... |EXT_POWER_DOWN
```


02/11/21
19:40:00

ttyaudit-ttyS0-20210211-190608.log

3

```
2021-02-11T19:07:40+0000 ttyS0 DES POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running Triple DES POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Triple DES POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running AES POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 AES POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running SHA1 POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 SHA1 POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running SHA2 POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 SHA2 POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running RandomGen POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 RandomGen POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running RSA POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 RSA POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running DSA POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 DSA POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Running ECC POST Test
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 ECC POST Test Passed
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0 Audit on 11/2/2021 17:20:20 00100008
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:40+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Keyper 9860-2 Serial Number H1411006
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Memory Usage:
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 RAM (free/total) 197Mb/256Mb
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Flash (free/total) 127Mb/128Mb
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 black store 440b
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 statistics 112b
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 other 116b
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 RedStore (free/total) 109Kb/128Kb
```

```
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Network Configuration:
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 IPv4: enabled
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 IPv6: enabled
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 MAC/IP address(es): 00:E0:06:C0:E3:1B / 192.168.0.2/24 , 2001::2e0:6ff:fec0:b31b/64
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 HSM Port: 05000
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 HSM Gateway(s): 0.0.0.0 ::
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Software Versions:
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 BBL 010 ABL 011 App 023
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 CPLD Version:
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 1.9
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 SCR Firmware Version:
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 OROS-R2.99-R1.20
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 HmcListener: Created IPv4 socket 10 on port 3000.
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 HmcListener: Created IPv6 socket 11 on port 3000.
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Audit on 11/2/2021 17:20:21 00100003
2021-02-11T19:07:41+0000 ttyS0
2021-02-11T19:07:41+0000 ttyS0 Audit on 11/2/2021 17:26:00 0020006a
2021-02-11T19:13:21+0000 ttyS0
2021-02-11T19:13:21+0000 ttyS0 Audit on 11/2/2021 17:26:40 00200069 0A400000B686296E
2021-02-11T19:14:00+0000 ttyS0
2021-02-11T19:14:00+0000 ttyS0
2021-02-11T19:14:27+0000 ttyS0 Audit on 11/2/2021 17:27:07 00200069 0A4000009D86296E
2021-02-11T19:14:27+0000 ttyS0
2021-02-11T19:14:27+0000 ttyS0
2021-02-11T19:14:56+0000 ttyS0 Audit on 11/2/2021 17:27:36 00200069 0A4000009DC6296E
2021-02-11T19:14:56+0000 ttyS0
2021-02-11T19:14:58+0000 ttyS0
2021-02-11T19:14:58+0000 ttyS0
2021-02-11T19:14:58+0000 ttyS0
2021-02-11T19:14:58+0000 ttyS0 TcpListener: Created IPv4 socket 15 on port 5000.
2021-02-11T19:14:58+0000 ttyS0
```

02/11/21
19:40:00

ttyaudit-ttyS0-20210211-190608.log

5

```
2021-02-11T19:14:58+0000 ttyS0
2021-02-11T19:14:58+0000 ttyS0
2021-02-11T19:14:58+0000 ttyS0 TcpListener: Created IPv6 socket 16 on port 5000.
2021-02-11T19:14:58+0000 ttyS0
2021-02-11T19:14:59+0000 ttyS0 Audit on 11/2/2021 17:27:39 00100002
2021-02-11T19:14:59+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:19:15+0000 ttyS0 TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2021-02-11T19:19:15+0000 ttyS0
2021-02-11T19:23:11+0000 ttyS0
2021-02-11T19:23:11+0000 ttyS0
2021-02-11T19:23:11+0000 ttyS0 CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2021-02-11T19:23:11+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:26:23+0000 ttyS0 TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2021-02-11T19:26:23+0000 ttyS0
2021-02-11T19:28:03+0000 ttyS0
2021-02-11T19:28:03+0000 ttyS0
2021-02-11T19:28:03+0000 ttyS0 CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2021-02-11T19:28:03+0000 ttyS0
2021-02-11T19:28:03+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0 TcpListener: Accepted connection on socket 14 from address 192.168.0.1.
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0 CryptoTask: Closing connection on socket 14 from address 192.168.0.1.
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:30:15+0000 ttyS0 TcpListener: Accepted connection on socket 17 from address 192.168.0.1.
2021-02-11T19:30:15+0000 ttyS0
2021-02-11T19:31:47+0000 ttyS0
2021-02-11T19:31:47+0000 ttyS0
2021-02-11T19:31:47+0000 ttyS0 CryptoTask: Closing connection on socket 17 from address 192.168.0.1.
2021-02-11T19:31:47+0000 ttyS0
2021-02-11T19:31:47+0000 ttyS0
2021-02-11T19:38:37+0000 ttyS0 Audit on 11/2/2021 17:51:17 0020006a
2021-02-11T19:38:37+0000 ttyS0
2021-02-11T19:39:03+0000 ttyS0 Audit on 11/2/2021 17:51:43 00200069 0A400000B686296E
```

02/11/21
19:40:00

ttyaudit-ttyS0-20210211-190608.log

6

```
2021-02-11T19:39:03+0000 ttyS0
2021-02-11T19:39:30+0000 ttyS0 Audit on 11/2/2021 17:52:10 00200069 0A4000009D86296E
2021-02-11T19:39:30+0000 ttyS0
2021-02-11T19:39:56+0000 ttyS0 Audit on 11/2/2021 17:52:36 00200069 0A4000009DC6296E
2021-02-11T19:39:56+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0 TcpListener: Closed IPv4 socket 15 on port 5000.
2021-02-11T19:40:00+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0 TcpListener: Closed IPv6 socket 16 on port 5000.
2021-02-11T19:40:00+0000 ttyS0
2021-02-11T19:40:00+0000 ttyS0 Audit on 11/2/2021 17:52:40 00100003
2021-02-11T19:40:00+0000 ttyS0
```

Print Logging Information

Step	Activity	Initials	Time
15	<p>CA executes the following commands using the terminal window to print a copy of the logging information:</p> <p>a) <code>lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true</code></p> <p>b) <code>enscript -2Gr script-202102*.log</code></p> <p>c) <code>enscript -Gr --font="Courier8" ttyaudit-tty*-202102*.log</code></p> <p>Attach the printed copies to IW script. Note: Ignore the error regarding non-printable characters if prompted.</p>	YG.	20:01

Place HSMFDs and OS DVDs into a TEB


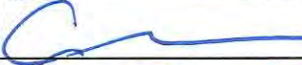

Step	Activity	Initials	Time
16	<p>CA executes the following commands using the terminal window to unmount the HSMFD:</p> <p>a) <code>cd /tmp</code></p> <p>b) <code>umount /media/HSMFD</code></p> <p>CA removes the HSMFD, then places it on the holder.</p>	YG.	20:01
17	<p>CA performs the following steps to switch OFF the laptop and remove the OS DVD:</p> <p>a) Remove the OS DVD from the laptop.</p> <p>b) Turn OFF the laptop by pressing the power button.</p> <p>c) Disconnect all connections from the laptop.</p>	YG.	20:02
18	CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it.	YG.	20:04
19	<p>CA performs the following steps to verify the TEB:</p> <p>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.</p> <p>b) Confirm with IW that the TEB number matches with the information below.</p> <p>c) Initial the TEB along with IW using a ballpoint pen.</p> <p>d) Give IW the sealing strips for post-ceremony inventory.</p> <p>e) Place the OS DVD TEB on the cart.</p> <p>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951322 ✓</p>	YG.	20:05
20	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	YG.	20:05

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.	YG	20:07
22	<p>CA performs the following steps:</p> <p>a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see.</p> <p>b) Confirm with IW that the TEB number and laptop serial number matches with the information below.</p> <p>c) Initial the TEB along with IW using a ballpoint pen.</p> <p>d) Give IW the sealing strips for post-ceremony inventory.</p> <p>e) Place the laptop TEB on the cart.</p> <p>Laptop4: TEB # BB81420089 / Service Tag # F8SVSG2 ✓</p>	YG	20:08

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
23	<p>CA perform the following steps sequentially for the COs listed below:</p> <p>a) Gather the OP TEB and plastic case prepared for the CO.</p> <p>b) Take the CO's OP card from the card holder and place it inside of the plastic case.</p> <p>c) Place the plastic case into the prepared TEB, read aloud the TEB number and description, then seal it.</p> <p>d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory.</p> <p>e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.</p> <p>f) IW writes the date and time, then signs the table of IW's script, then CA initials the entry.</p> <p>g) IW places the TEBs on the ceremony table.</p> <p>h) Repeat steps for the remaining COs' credentials on the list.</p> <p>CO4: Carlos Martinez OP TEB # BB91951297 ✓</p> <p>CO5: Olafur Gudmundsson OP TEB # BB91951296 ✓</p> <p>CO6: Nicolas Antonello OP TEB # BB91951295 ✓</p>	YG	20:17

CO	Card Type	TEB #	Printed Name	Signature	Date	Time	CA Initials
CO4	OP 4 of 7	OP TEB # BB91951297	Yuko Green		2021 Feb 14	20:12	FA
CO5	OP 5 of 7	OP TEB # BB91951296	Yuko Green		2021 Feb 11	20:15	FA
CO6	OP 6 of 7	OP TEB # BB91951295	Yuko Green		2021 Feb 11	20:17	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.)	YG.	20:18
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 at the first number in the combination.	YG.	20:19
26	SSC1 removes the safe log, then writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	YG.	20:20
27	CA performs the following steps to return each piece of equipment to the safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where "Return" is indicated. d) IW verifies the safe log entry, then initials it. HSM4: TEB # BB51184285 ✓ Laptop4: TEB # BB81420089 ✓ OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951322 ✓	YG.	20:22

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
28	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the entry, then initials it.	YG.	20:23
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.	YG.	20:23
30	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	YG.	20:24

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.)	YG.	20:25
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 at the first number in the combination.	YG.	20:26
33	SSC2 removes the safe log, then writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	YG.	20:26

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

Step	Activity	Initials	Time
34	<p>IW performs the following steps sequentially to return the required TEBs:</p> <p>a) IW reads aloud the TEB number, then verifies the integrity of the TEB while showing it to the audit camera above</p> <p>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.</p> <p>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.</p> <p>d) IW writes the date and time, then signs the safe log where "Return" is indicated.</p> <p>e) CA verifies the completed safe log entry, then initials it.</p> <p>CO4: Carlos Martinez Box # 1068 OP TEB # BB91951297</p> <p>CO5: Olafur Gudmundsson Box # 1789 OP TEB # BB91951296</p> <p>CO6: Nicolas Antonello Box # 1073 OP TEB # BB91951295</p>	YG.	20:32

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
35	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the safe log entry, then initials it.	YG.	20:32
36	SSC2 returns the safe log back to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	YG.	20:33
37	CA, IW, and SSC2 leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	YG.	20:33

Place Crypto Officer Keys into TEBs

Step	Activity	Initials	Time
38	<p>CA performs the following steps sequentially for the COs key listed below:</p> <ul style="list-style-type: none"> 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. <p>CO4: Carlos Martinez Key TEB # BB91951299 ✓</p> <p>CO5: Olafur Gudmundsson Key TEB # BB91951298 ✓</p> <p>CO6: Nicolas Antonello Key TEB # BB91951293 ✓</p> <p>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.</p>	YGT	20:42

Crypto Officer Safe Deposit Box Key Declaration

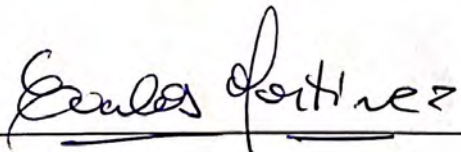
Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Carlos Martinez** hereby attest that my safe deposit box key for safe deposit box #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 #BB91951329** before transmitting the key via courier.

I witnessed the key's 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 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 #BB91951299** 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 MARTINEZ

Signature 

Date 24/02/2021

Crypto Officer Safe Deposit Box Key Declaration

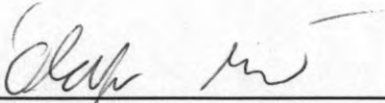
Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Olafur Gudmundsson** hereby attest that my safe deposit box key for safe deposit 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 #BB91951327** before transmitting the key via courier.

I witnessed the key's 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 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 #BB91951298** 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 OLAFUR GUDMUNDSSON

Signature 

Date 2021/2/24

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 Antonello** 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 #BB91951323** before transmitting the key via courier.

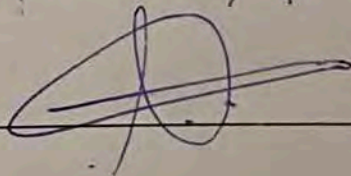
I witnessed the key's extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization 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 #BB91951293** 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 Antonello

Signature _____



Date _____

18/FEB/2021

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 #BB91951330** before transmitting the key via courier.

I attest the safe deposit box key was returned to me in the same sealed TEB 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 S D

Date 16/JAN/2021

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.	YG.	20:42
2	CA asks any COs who are participating remotely if they have any concerns pertaining to the ceremony or exceptions which may have occurred.	YG.	20:43
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.	YG.	20:44
4	CA reviews IW's script, then signs the participants list.	YG.	20:46
5	IW signs the list and records the completion time.	YG.	20:46

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.	YG.	20:47
7	CA informs onsite participants of post ceremony activities.	YG.	20:47
8	Ceremony participants take a group photo.	YG.	20:53
9	CA acknowledges the participation of the COs, RZM, and Auditors in the call, then stops the call.	YG.	20:53

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.)	YG.	21:12
11	CA requests that an SA stop the audit camera video recording.	YG.	20:54

Bundle Audit Materials

Step	Activity	Initials	Time
12	<p>IW makes a copy of their script for off-site audit bundle containing:</p> <ul style="list-style-type: none"> 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: 20200423 00:00:00 to 20210212 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). <p>All TEBs are labeled Root DNSSEC KSK Ceremony 42, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>	YG.	U=30

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-256 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 footage - 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 with this script.
Any exceptions that occurred were accurately and properly documented.

IW: **Yuko Green**

Signature: 

Date: 2021 Feb 11

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 in 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: **20200423 00:00:00 to 20210212 00:00:00 UTC.**

SA:

Patrick Tudor

Signature:



Date: 2021 Feb 11

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 6th Edition (2020-11-04). No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

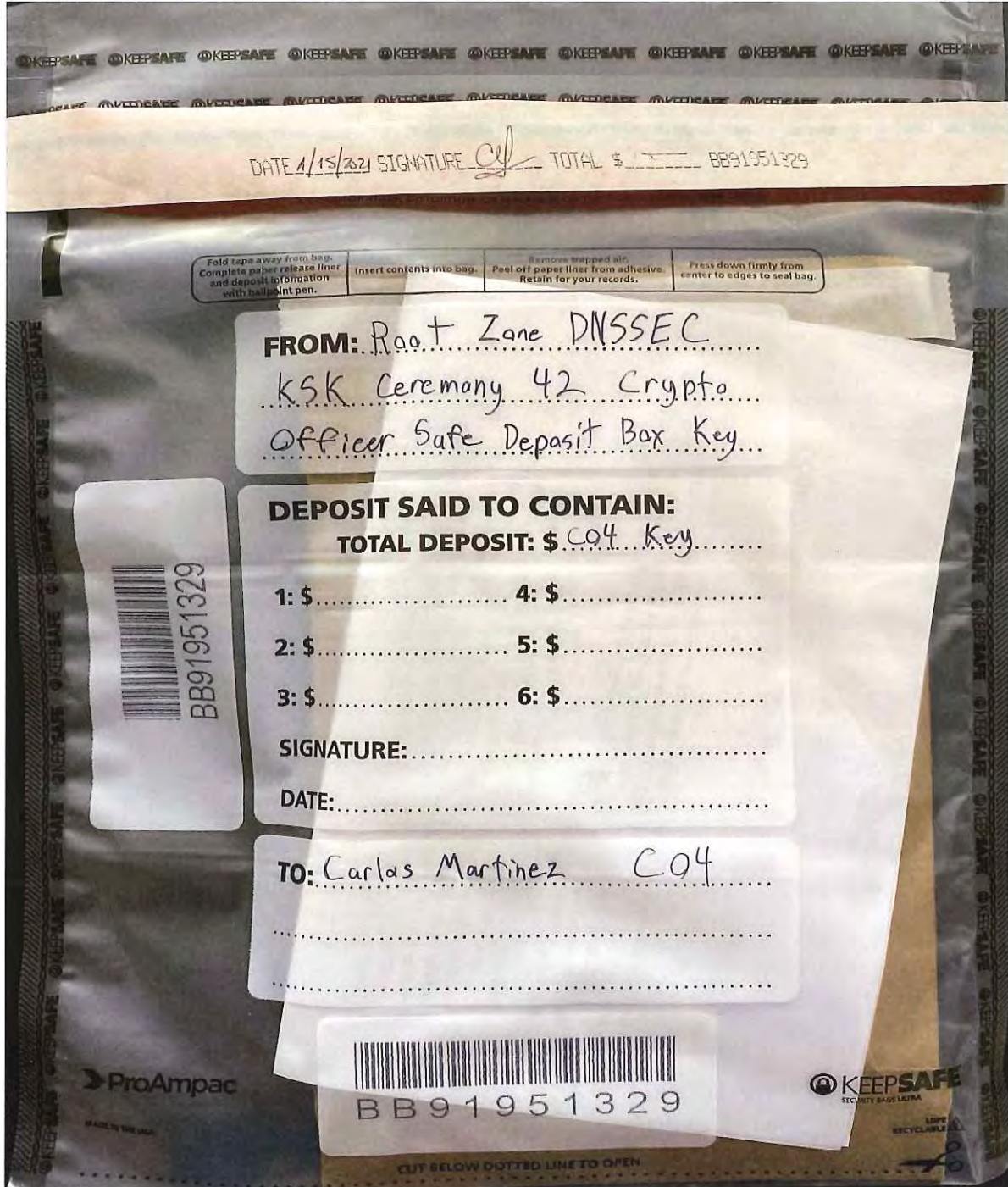
SA: Patrick L Tudor

Signature: 

Date: 2021 Feb 11

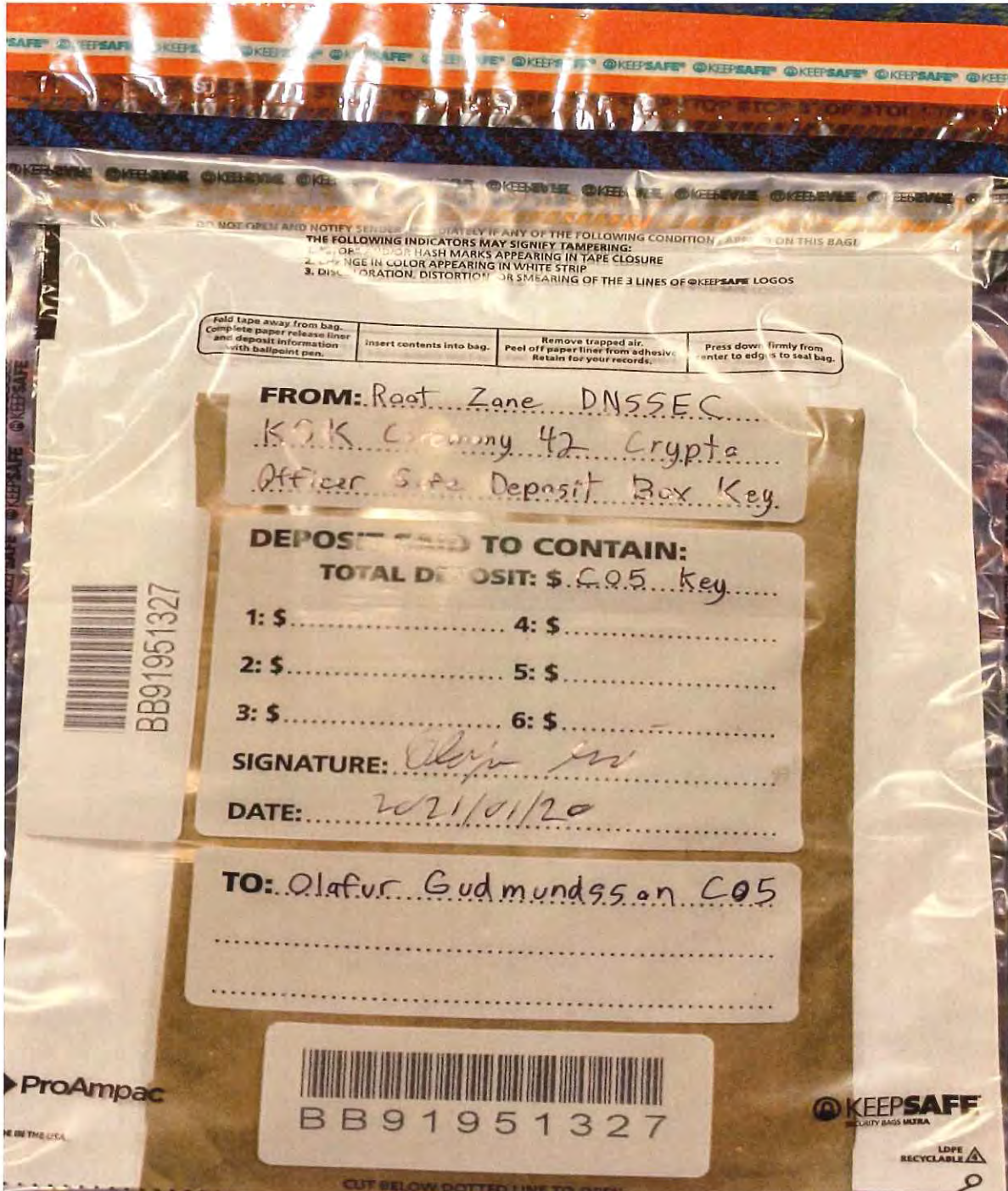
Appendix F: CO4 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO4 Carlos Martinez** Safe Deposit Box Key **TEB # BB91951329** dispatched from the CO.



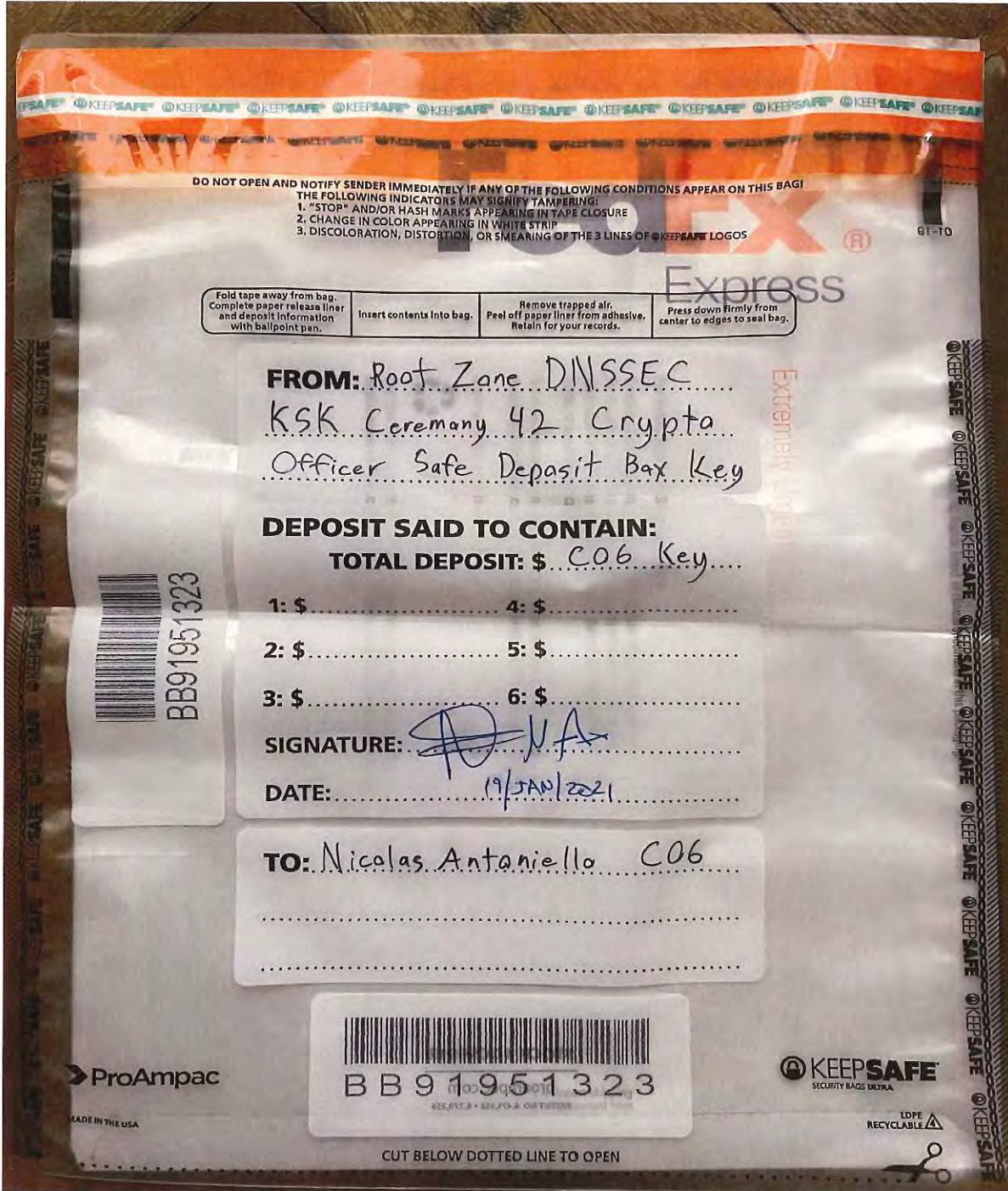
Appendix G: CO5 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO5 Olafur Gudmundsson Safe Deposit Box Key TEB # BB91951327** dispatched from the CO.



Appendix H: CO6 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO6 Nicolas Antonello Safe Deposit Box Key TEB # BB91951323** 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 # BB91951330** 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 "XXXXXX"; ## SECRET-DATA
  }
  name-server {
    192.0.42.53;
  }
  login {
    user bmartin {
      full-name "Brian Martin";
      uid 2005;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## SECRET-DATA
      }
    }
    user cbarthold {
      full-name "Connor A. Barthold";
      uid 2004;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## SECRET-DATA
      }
    }
    user dkara {
      full-name "Darren Kara";
      uid 2001;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## SECRET-DATA
      }
    }
    user jjenkins {
      full-name "Josh Jenkins";
      uid 2007;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## SECRET-DATA
      }
    }
    user ptudor {
      full-name "Patrick Tudor";
      uid 2000;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## SECRET-DATA
      }
    }
    user rquinn {
      full-name "Reed Quinn";
      uid 2003;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## SECRET-DATA
      }
    }
    user sfreeark {
      uid 2002;
      class super-user;
      authentication {
        encrypted-password "XXXXXX"; ## 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-rollback 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 {

```

