Root DNSSEC KSK Ceremony 50

Wednesday 19 July 2023

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

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

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 1 Step(s): 2 Page(s): 5 Date and Time: 19 July 2023 @ 20:02 **Note: IW describes the exception(s) and action(s) below.**	A.A.	20:02

Danielle Gordon, a staff witness, is absent.

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	Gustavo Lozano / ICANN		2023 Jul 19	23:44
IW	Yuko Yokoyama / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Anand Mishra / ICANN			
CO1	Arbogast Fabian			
CO2	Ralf Weber			
CO3	João Damas			
CO6	Jorge Etges			
CO7	Subramanian Moonesamy			
RZM	Duane Wessels / Verisign			
AUD	Kacie Bellisch / RSM			
AUD	Paul M. Lee / RSM			
SA	Moises Cirilo / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
~~SW~~	~~Danielle Gordon / ICANN~~			
SW	Michelle Wilson / ICANN			
SW	Natalie Schoer / ICANN			
EW	Jonathan Moura Jones / Global Media Desk			
EW	Alejandro Gatti / Global Media Desk			
EW	Shawn Hood			
EW	Henry Magalong			

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 and COs into Tier 5 (Safe Room) to retrieve the following materials:

- Safe #1: HSM, laptop, OS media, etc
- Safe #2: The COs' cards 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.	Y.Y.	20:00
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.	Y.Y.	20:03
3	CA asks that any first time ceremony participants in the room introduce themselves.	Y.Y.	20:04

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.	Y.Y.	20:04
5	CA explains the use of personal electronic devices during the ceremony.	Y.Y.	20:05
6	CA summarizes the purpose of the ceremony.	Y.Y.	20:06

Verify the Time and Date

Step	Activity	Initials	Time
7	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: 2023-07-19 20:07 **Note: All entries into this script or any logs should follow this common source of time.**	Y.Y	20:07

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
8	CA transports the guard key and flashlight, and with IW escorts SSC2 and the COs into Tier 5 (Safe Room.)	Y.Y.	20:08
9	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.**	Y.Y.	20:10
10	Perform the following steps to complete the safe log: a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies the entry then initials it.	Y.Y.	20:11

COs Access the Credentials in Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
11	COs perform the following steps sequentially to access the listed TEBs: a) After the CA operates the guard key in the bottom lock, CO reads aloud their safe deposit box number then uses their tenant key to operate the top lock. b) CO opens their safe deposit box, verifies its integrity, then removes the TEBs. c) CO reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above. d) CO performs the actions specified below, then locks their safe deposit box. e) CO writes the date and time, then signs the safe log. f) IW verifies the completed safe log entries, then initials them. **CO1: Arbogast Fabian** **Box # 1788** **OP TEB # BB91951310** (Retain)✓ **SO TEB # BB91951309** (Retain) ✓ **Set # 1 TEB # BB02638562** (Retain) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **Set # 2 TEB # BB02638561** (Check and Return)✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO2: Ralf Weber** **Box # 1071** **OP TEB # BB02638566** (Retain) ✓ **SO TEB # BB02638565** (Retain) ✓ **Set # 1 TEB # BB02638560** (Retain) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **Set # 2 TEB # BB02638559** (Check and Return) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO3: João Damas** **Box # 1069** **OP TEB # BB91951308** (Retain) ✓ **SO TEB # BB91951307** (Retain) ✓ **Set # 1 TEB # BB02638558** (Retain) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **Set # 2 TEB # BB02638557** (Check and Return) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO6: Jorge Etges** **Box # 1072** **OP TEB # BB91951306** (Retain)✓ **SO TEB # BB91951305** (Retain)✓ **Set # 1 TEB # BB02638552** (Retain)✓ Last Verified: KSK Ceremony 48 2023-02-01 **Set # 2 TEB # BB02638551** (Check and Return)✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO7: Subramanian Moonesamy** **Box # 1790** **OP TEB # BB91951304** (Retain) ✓ **SO TEB # BB91951303** (Retain)✓ **Set # 1 TEB # BB02638550** (Retain) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **Set # 2 TEB # BB02638549** (Check and Return)✓ Last Verified: KSK Ceremony 48 2023-02-01 **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.**	Y.Y.	20:26

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
12	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry then initials it.	Y.Y.	20:27
13	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	Y.Y.	20:27
14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	Y.Y.	20:28

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
15	CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.)	Y.Y.	20:29
16	SSC1 opens Safe #1 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.**	Y.Y.	20:29
17	Perform the following steps to complete the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies the entry then initials it.	Y.Y.	20:30

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

Step	Activity	Initials	Time
18	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified in the list below. d) Write the date and time, then signs the safe log. e) IW verifies the completed safe log entries, then initials it. **HSM5W: TEB # BB51184248 (Place on Cart)** ✓ Last Verified: KSK Ceremony 46 2022-08-17 **HSM6W: TEB # BB51184545 (Place on Cart)** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **HSM7W: TEB # BB51184520 (Place on Cart)** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **Laptop3: TEB # BB97448420 (Check and Return)** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **Laptop4: TEB # BB81420086 (Place on Cart)** ✓ Last Verified: KSK Ceremony 46 2022-08-17 **OS media (release coen-0.4.0) + HSMFD: TEB # BB02638569 (Place on Cart)** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **KSK-2017: TEB # BB02638568 (Check and Return)** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **KSK-2023: TEB # BB02638527 (Place on Cart)** ✓ Last Verified: KSK Ceremony 49 2023-04-27 / KSK Media Deposit 49 2023-04-29 **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.**	Y.Y.	20:36

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

Step	Activity	Initials	Time
19	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry then initials it.	Y.Y.	20:37
20	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	Y.Y.	20:37
21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	Y.Y.	20:38

Act 2: Introduce New OS Media

The CA will introduce new OS media by performing the following steps:

- Verify the new OS media matches the checksum published online at https://github.com/iana-org/coen
- Calculate new OS media checksums using the current OS media. Once the new OS media hash has been verified it will be ready to use in production to perform the ceremony
- Discard previous OS media after new OS media has been verified

Laptop Setup

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the listed equipment: a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **Laptop4: TEB # BB81420086 / Service Tag # F8SVSG2** ✓ Last Verified: KSK Ceremony 46 2022-08-17 **OS media (release coen-0.4.0) + HSMFD: TEB # BB02638569** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **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.**	Y.Y.	20:42
2	CA performs the following steps to confirm that no hard drive and battery are in the laptop: a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty.	Y.Y.	20:43
3	CA performs the following steps to boot the laptop: a) Connect the external HDMI display cable. b) Connect the power supply. c) Immediately insert the **OS media release coen-0.4.0** after the laptop power is switched ON.	Y.Y.	20:46
4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	Y.Y.	20:46

OS Media Checksum Verification

Step	Activity	Initials	Time
	CA uses the terminal window to executes the following steps: a) Calculate the SHA-256 hash by executing: `sha2wordlist < /dev/sr0` b) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.**	Y.Y.	20:48
5	SHA-256 hash: **8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f** PGP Words: **minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document** **Note: The SHA-256 hash of the OS media release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/50**		

OS DVD Acceptance Test

Step	Activity	Initials	Time
6	CA connects the external DVD drive to the USB port of the laptop.	Y.Y.	20:49

7	CA inserts the new **OS media release coen-1.0.0** DVD into the external DVD drive, waits for it to be recognized by the OS, then performs the following steps:
	a) Close the file system popup window.
	CA uses the terminal window to continues with the following steps:
	b) Confirm the drive letter by executing:
	`lsblk`
	c) Verify the byte count of the DVD matches the **OS media release coen-1.0.0** ISO size of **375431168** by running the following command:
	`df -B1 /dev/sr1`
	d) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sr1 | sha2wordlist`
	e) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.
	f) Unmount the drive by executing:
	`umount /dev/sr1`
	
	SHA-256 hash:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/50
		Y.Y.	20:53

8	CA removes the new OS media DVD by pressing the eject button on the external DVD drive, then places it on the ceremony table. **Note: The tested OS media must be placed on the ceremony table where it is visible to the audit camera and the participants**	Y.Y.	20:54
9	CA repeats step 7 to 8 for the 2nd copy of the new **OS media release coen-1.0.0**.	Y.Y.	20:57
10	CA disconnects the external DVD drive from the laptop.	Y.Y.	20:57

OS SD Card Acceptance Test

Step	Activity	Initials	Time
11	CA ensures the **lock switch** on the left side of the SD card is slid down to the lock position.	Y.Y.	20:58

12	CA inserts the new **OS media release coen-1.0.0** SD card into the SD card drive, then performs the following steps using the terminal window:
	a) Confirm the drive letter by executing:
	`lsblk`
	b) Mount the drive by executing:
	`mount /dev/sda /mnt`
	c) Verify the byte count of the SD card matches the **OS media release coen-1.0.0** ISO size of **375431168** by running the following command:
	`df -B1 /dev/sda`
	d) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sda | sha2wordlist`
	e) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.
	f) Unmount the drive by executing:
	`umount /dev/sda`
	
	SHA-256 hash:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/50
		Y.Y.	21:01

13	CA removes the new OS media SD card, then places it on the ceremony table. **Note: The tested OS media must be placed on the ceremony table where it is visible to the audit camera and the participants**	Y.Y.	21:01
14	CA repeats step 11 to 13 for the 2nd copy of the new **OS media release coen-1.0.0** SD card.	Y.Y.	21:03

Retire Previous OS Media

Step	Activity	Initials	Time
15	CA performs the following steps to switch OFF the laptop and remove the OS media: a) Remove the OS media from the laptop. b) Turn OFF the laptop by pressing the power button. c) Disconnect all connections from the laptop. d) Discard all copies of the **OS media release coen-0.4.0**.	Y.Y.	21:04

Act 3: Equipment Setup

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

- Boot the laptop using the OS media (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	CA performs the following steps to prepare the listed equipment: a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM5W: TEB # BB51184248 ✓ / Serial # H1903017 ✓** Last Verified: KSK Ceremony 46 2022-08-17 **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.**	Y.Y.	21:08
2	CA ensures the **lock switch** on the left side of the listed SD card is slid down to the lock position: **OS media release coen-1.0.0** **Copy # 1**	Y.Y.	21:09
3	CA performs the following steps to boot the laptop: a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into a USB port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Insert the **OS media release coen-1.0.0 Copy # 1**. f) Switch it ON.	Y.Y.	21:12
4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	Y.Y.	21:12

OS Media Checksum Verification

Step	Activity	Initials	Time

5	CA uses the terminal window to executes the following steps:
	a) Verify the byte count of the SD card matches the **OS media release coen-1.0.0** ISO size of **375431168** by running the following command:
	`df -B1 /dev/sda`
	b) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sda | sha2wordlist`
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.
	
	SHA-256 hash:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/50
		Y.Y.	21:13

Printer Setup

Step	Activity	Initials	Time
6	CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page: `configure-printer`	Y.Y.	21:14

Date Setup

Step	Activity	Initials	Time
7	CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock. If the date/time do not match, perform the following steps: a) Execute `date -s "20230719 HH:MM:00"` to set the time. **where `HH` is two-digit hour, `MM` is two-digit minutes and `00` is zero seconds.** b) Execute `date` to confirm the date/time matches the clock.	Y.Y.	21:14

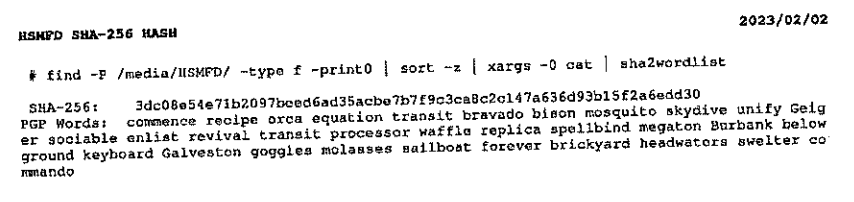
Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 3 Step(s): 9 Page(s): 16 Date and Time: 19 July 2023 @ 21:19 **Note: IW describes the exception(s) and action(s) below.**	Y.Y.	21:19

The ceremony 48 annotated script was not available. We verified the result against the printed copy from the safe.

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the **Ceremony 48 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.	Y.Y.	21:14
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash -c` CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script.  HSMFD SHA-256 HASH 2023/02/02 # find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist SHA-256: 3dc08e54e71b2097beed6ad35acbe7b7f9c3ca8c2c147a636d93b15f2a6edd30 PGP Words: commence recipe orca equation transit bravado bison mosquito skydive unify Geiger sociable enlist revival transit processor waffle replica spellbind megaton Burbank below ground keyboard Galveston goggles molasses sailboat forever brickyard headwaters swelter commando IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 48 annotated script.	Y.Y.	21:18

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 48** and the sheet of paper with the printed HSMFD hash to RKOS.	Y.Y.	21:21

Start the Terminal Session Logging

Step	Activity	Initials	Time
11	CA executes the command below using the terminal window to change the working directory to HSMFD: `cd /media/HSMFD`	Y.Y.	21:21
12	CA executes the command below to log activities of the **Commands** terminal window: `script script-20230719.log`	Y.Y.	21:21

Start the HSM Output Logging

Step	Activity	Initials	Time

13	CA performs the following steps using the **HSM Output** terminal window to capture the activity logs of the HSM:
	a) Change the working directory to HSMFD by executing:
	`cd /media/HSMFD`
	b) Set the serial port baud rate by executing:
	`stty -F /dev/ttyUSB0 115200`
	c) Start logging the serial output by executing:
	`ttyaudit /dev/ttyUSB0`
	Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.
		Y.Y.	21:22

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM5W**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. **Note: Status information should appear in the HSM output logging screen.** d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H1903017**. e) Scroll down to the end of the logging screen. **HSM5W: Serial # H1903017** ✓ **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	Y.Y.	21:24

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 4 Step(s): 1 Page(s): 18 Date and Time: 19 July 2023, 21:40 **Note: IW describes the exception(s) and action(s) below.**	Y.Y.	21:40

For CO1 Arbogast Fabien and CO6 Jorge Etges, their OP and SO TEBs were verified against the ceremony 4b script.

Act 4: Activate HSM (Tier 7) and Generate Signatures

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

- The CA activates the HSM using the COs' cards
- After connectivity is confirmed the flash drive containing the KSRs is inserted into the laptop
- The ksr signer application uses the private key stored in the HSM to generate the SKRs containing the digital signatures of the ZSK slated for future use
- The CA then prints the signer log, backs up the newly created SKRs, and deactivates the HSM

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
1	The CA calls each of the COs listed below sequentially to perform the following steps: a) CO reads aloud the TEB number, then CA inspects it for tamper evidence while IW verifies the information using the previous ceremony script where it was last used. b) CO and CA open the TEB, then the CA removes the plastic case containing the cards as specified below. **CO1: Arbogast Fabian** **OP TEB # BB91951310** (Place the plastic case on the table for destruction) ✓ **SO TEB # BB91951309** (Place the plastic case on the table for destruction) ✓ **Set # 1 TEB # BB02638562** (Place the cards on the designated card holder) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO2: Ralf Weber** **OP TEB # BB02638566** (Place the plastic case on the table for destruction) ✓ **SO TEB # BB02638565** (Place the plastic case on the table for destruction) ✓ **Set # 1 TEB # BB02638560** (Place the cards on the designated card holder) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO3: João Damas** **OP TEB # BB91951308** (Place the plastic case on the table for destruction) ✓ **SO TEB # BB91951307** (Place the plastic case on the table for destruction) ✓ **Set # 1 TEB # BB02638558** (Place the cards on the designated card holder) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO6: Jorge Etges** **OP TEB # BB91951306** (Place the plastic case on the table for destruction) ✓ **SO TEB # BB91951305** (Place the plastic case on the table for destruction) ✓ **Set # 1 TEB # BB02638552** (Place the cards on the designated card holder) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **CO7: Subramanian Moonesamy** **OP TEB # BB91951304** (Place the plastic case on the table for destruction) ✓ **SO TEB # BB91951303** (Place the plastic case on the table for destruction) ✓ **Set # 1 TEB # BB02638550** (Place the cards on the designated card holder) ✓ Last Verified: KSK Ceremony 48 2023-02-01 **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.**	Y.Y.	21:38

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards.	Y.Y.	21:45
2	Confirm the **"READY"** LED on the **HSM** is **ON.** IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st OP card 1 of 7 2nd OP card 2 of 7 3rd OP card 3 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**		

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.	Y.Y.	21:44

4	CA performs the following steps to test the network connectivity between laptop and HSM:
	a) Use the **Commands** terminal window
	b) Test connectivity by executing:
	`ping hsm`
	c) Wait for responses, then exit by pressing:
	`Ctrl + C`
		Y.Y.	21:46

Insert the KSRFD

Step	Activity	Initials	Time
5	CA plugs the **KSRFD** 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 1 KSR.**	Y.Y.	21:47

Execute the KSR Signer for KSR 2023 Q4

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSRFD/KSK50/ksr-root-2023-q4-0.xml`	Y.Y.	21:48
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.	Y.Y.	21:48

July 18, 2023

VERISIGN

To Whom It May Concern:

This is a letter of Verification of Employment for Duane Wessels. VeriSign, Inc. ("Verisign") has employed Duane Wessels full-time/40 hours per week since January 11, 2010, currently as a Fellow in Verisign's Platform Management department.

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 26 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for millions of .com and .net domain names and processing billions of 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,

X Dave Carney July 18, 2023

Dave Carney
HR Specialist - Verisign

Dave Carney | HR Specialist - Verisign | dcarney@verisign.com | (703) 948-4143

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

19 July 2023

The SHA256 hash of the 2023 Q4 KSR file is:

ksr-root-2023-q4-0.xml:

f139e2a852d76ee6c5e83c880c3308901358f87507f5e25cd79372c3142695c9

The PGP wordlist for the hash above is:

unwind corporate tiger paramount Dupont stethoscope goldfish trombonist solo typewriter cobra maritime ammo concurrent aimless millionaire Aztec everyday Vulcan impartial ahead visitor tiger fascinate stopwatch molasses highchair replica baboon caretaker preclude retrospect

Attested on behalf of VeriSign by:

Duane Wessels
Fellow
Naming Operations
VeriSign, Inc.

Verify the KSR Hash for KSR 2023 Q4

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed in the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification **off camera** for the purpose of authentication while maintaining privacy. **Note: If the RZM representative is not physically present in the room, write the representative's name and *"Remote Participant"* next to the name on the signature line.** b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line: **Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS in advance to be included in the final annotated script and audit bundle.** Duane Wessels c) The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.	Y.Y.	21:50
9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**	Y.Y.	21:51
10	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in: `/media/KSRFD/KSK50/skr-root-2023-q4-0.xml`	Y.Y.	21:51

Print Copies of the KSR Signer Log

Step	Activity	Initials	Time
11	CA executes the commands below using the terminal window to print the KSR Signer log: a) `printlog ksrsigner-202307*.log X` **Note: Replace "X" with the amount of copies needed for the participants.**	Y.Y.	21:51
12	IW attaches a copy of the required ksr signer log to their script.	Y.Y.	21:51

Execute the New KSR Signer for KSR 2023 Q4

Step	Activity	Initials	Time
13	CA executes the command below in the terminal window to change directory: `cd /media/KSRFD/KSK50/new/`	Y.Y.	21:52
14	CA executes the command below in the terminal window to sign the KSR file: `kskm-ksrsigner`	Y.Y.	21:52

```
Starting: ksrsigner /media/KSRFD/KSK50/ksr-root-2023-q4-0.xml (at Wed Jul 19 21:47:50 2023 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1903017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-07-01T00:00:00 2023-07-22T00:00:00  11019,60955   20326(Klajeyz)/S
2  2023-07-11T00:00:00 2023-08-01T00:00:00  11019         20326(Klajeyz)/S
3  2023-07-21T00:00:00 2023-08-11T00:00:00  11019         20326(Klajeyz)/S
4  2023-07-31T00:00:00 2023-08-21T00:00:00  11019         20326(Klajeyz)/S
5  2023-08-10T00:00:00 2023-08-31T00:00:00  11019         20326(Klajeyz)/S
6  2023-08-20T00:00:00 2023-09-10T00:00:00  11019         20326(Klajeyz)/S
7  2023-08-30T00:00:00 2023-09-20T00:00:00  11019         20326(Klajeyz)/S
8  2023-09-09T00:00:00 2023-09-30T00:00:00  11019         20326(Klajeyz)/S
9  2023-09-19T00:00:00 2023-10-10T00:00:00  46780,11019   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSRFD/KSK50/ksr-root-2023-q4-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  46780,11019
2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780
3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780
4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780
5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780
6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780
7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780
8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780
9  2023-12-20T00:00:00 2024-01-10T00:00:00  46780,30903
...PASSED.

SHA256 hash of KSR:
F139E2A852D76EE6C5E83C880C3308901358F87507F5E25CD79372C3142695C9
>> unwind corporate tiger paramount Dupont stethoscope goldfish trombonist solo typewriter cobra mari
time ammo concurrent aimless millionaire Aztec everyday Vulcan impartial ahead visitor tiger fascinat
e stopwatch molasses highchair replica baboon caretaker preclude retrospect <<

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/KSRFD/KSK50/skr-root-2023-q4-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  46780,11019   20326(Klajeyz)/S
2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780         20326(Klajeyz)/S
3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780         20326(Klajeyz)/S
4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780         20326(Klajeyz)/S
5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780         20326(Klajeyz)/S
6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780         20326(Klajeyz)/S
7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780         20326(Klajeyz)/S
8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780         20326(Klajeyz)/S
9  2023-12-20T00:00:00 2024-01-10T00:00:00  30903,46780   20326(Klajeyz)/S

SHA256 hash of SKR:
4784544BD1E140A7DE787BD31B8DC884B269C63D8860401EBF91D63E2A7AB111
>> dashboard Jupiter eating disable stairway tolerance crackdown paragraph tactics indigo kickoff soc
iable beeswax microscope spaniel Jupiter sawdust guitarist southward crucifix newborn fortitude crack
down Burlington slingshot miracle stockman cumbersome brickyard infancy sailboat Babylon <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

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

19 July 2023

The SHA256 hash of the 2023 Q4 KSR file is:

ksr-root-2023-q4-0.xml:

f139e2a852d76ee6c5e83c880c3308901358f87507f5e25cd79372c3142695c9

The PGP wordlist for the hash above is:

unwind corporate tiger paramount Dupont stethoscope goldfish trombonist solo typewriter cobra maritime ammo concurrent aimless millionaire Aztec everyday Vulcan impartial ahead visitor tiger fascinate stopwatch molasses highchair replica baboon caretaker preclude retrospect

Attested on behalf of VeriSign by:

Duane Wessels
Fellow
Naming Operations
VeriSign, Inc.

Verify the KSR Hash for KSR 2023 Q4

Step	Activity	Initials	Time
15	The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.	Y.Y.	21:53
16	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**	Y.Y	21:53
17	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The SKR is located in: `/media/KSRFD/KSK50/new/`	Y.Y.	21:53

Print Copies of the New KSR Signer Log

Step	Activity	Initials	Time
18	CA executes the commands below using the terminal window to print the KSR Signer log: a) `printlog kskm-ksrsigner-202307*.log X` **Note: Replace "X" with the amount of copies needed for the participants.**	Y.Y.	21:54
19	IW attaches a copy of the required ksr signer log to their script.	Y.Y.	21:55

SKR Comparison

Step	Activity	Initials	Time
20	CA executes the commands below using the terminal window to compare the SKRs: a) `xsltproc style.xsl ../skr-root-2023-q4-0.xml | xmllint --format - > current` b) `xsltproc style.xsl skr-root-2023-q4-0-new.xml | xmllint --format - > new` c) `diff -wu current new`	Y.Y.	21:57
21	CA executes the command below in the terminal window to change directory: `cd /media/HSMFD`	Y.Y.	21:57

Copy the Newly Created SKR

Step	Activity	Initials	Time

22	CA executes the following commands using the terminal window:
	a) List the contents of the KSRFD by executing:
	`ls -ltrR /media/KSRFD`
	b) Copy the contents of the KSRFD to the HSMFD by executing:
	`cp -pR /media/KSRFD/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD by executing:
	`ls -ltrR`
	d) Verify it has been copied successfully by executing:
	`diff -qr /media/HSMFD/KSK50/ /media/KSRFD/KSK50/`
	e) Unmount the KSRFD by executing:
	`umount /media/KSRFD`
		Y.Y.	21:58

23	CA removes the **KSRFD** containing the SKR files, then gives it to the RZM representative. **Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.**	Y.Y.	21:59

```
Loaded configuration from file ksrsigner.yaml SHA-256 11e564d66bda046b76daac6311cf727391c13d06c41b554
8864818eb1ea88be6 WORDS Athens travesty flytrap speculate glitter surrender adrift Hamilton inverse s
urrender ribcage Galveston Athens Saturday highchair hurricane pheasant recover commence amulet snows
lide bravado edict dictator necklace dictator beaming underfoot berserk paramount obtuse trombonist
Configuration validated
Loaded SKR from file skr-root-2023-q3-0.xml SHA-256 063f6815afbf4f3676a6b9fdea52d0a66c370632463928c19
9ed5269d20468c5 WORDS afflict customer frighten bifocals rocker rebellion dropper congregate inverse
paragon sentence Wyoming Trojan enrollment stagnate paragon glucose consensus afflict component cubic
 corporate breadline recover prowler unify Dupont guitarist standard alkali frighten resistor
Previous SKR:
#  Inception           Expiration          ZSK Tags      KSK(CKA_LABEL)
1  2023-07-01T00:00:00 2023-07-22T00:00:00  60955,11019   20326(Klajeyz)/S
2  2023-07-11T00:00:00 2023-08-01T00:00:00  11019         20326(Klajeyz)/S
3  2023-07-21T00:00:00 2023-08-11T00:00:00  11019         20326(Klajeyz)/S
4  2023-07-31T00:00:00 2023-08-21T00:00:00  11019         20326(Klajeyz)/S
5  2023-08-10T00:00:00 2023-08-31T00:00:00  11019         20326(Klajeyz)/S
6  2023-08-20T00:00:00 2023-09-10T00:00:00  11019         20326(Klajeyz)/S
7  2023-08-30T00:00:00 2023-09-20T00:00:00  11019         20326(Klajeyz)/S
8  2023-09-09T00:00:00 2023-09-30T00:00:00  11019         20326(Klajeyz)/S
9  2023-09-19T00:00:00 2023-10-10T00:00:00  46780,11019   20326(Klajeyz)/S
Loaded KSR from file ksr-root-2023-q4-0.xml SHA-256 f139e2a852d76ee6c5e83c880c3308901358f87507f5e25cd
79372c3142695c9 WORDS unwind corporate tiger paramount Dupont stethoscope goldfish trombonist solo ty
pewriter cobra maritime ammo concurrent aimless millionaire Aztec everyday Vulcan impartial ahead vis
itor tiger fascinate stopwatch molasses highchair replica baboon caretaker preclude retrospect
Validating KSR using request policy:
  _dataclass_placeholder: None
  acceptable_domains: ['.']
  approved_algorithms: ['RSASHA256']
  check_bundle_intervals: True
  check_bundle_overlap: True
  check_chain_keys: True
  check_chain_keys_in_hsm: True
  check_chain_overlap: True
  check_cycle_length: True
  check_keys_match_ksk_operator_policy: True
  check_keys_publish_safety: True
  check_keys_retire_safety: True
  dns_ttl: 172800
  enable_unsupported_ecdsa: False
  keys_match_zsk_policy: True
  max_bundle_interval: 11 days, 0:00:00
  max_cycle_inception_length: 81 days, 0:00:00
  min_bundle_interval: 9 days, 0:00:00
  min_cycle_inception_length: 79 days, 0:00:00
  num_bundles: 9
  num_different_keys_in_all_bundles: 3
  num_keys_per_bundle: [2, 1, 1, 1, 1, 1, 1, 1, 2]
  rsa_approved_exponents: [65537]
  rsa_approved_key_sizes: [2048]
  rsa_exponent_match_zsk_policy: True
  signature_algorithms_match_zsk_policy: True
  signature_check_expire_horizon: True
  signature_horizon_days: 180
  signature_validity_match_zsk_policy: True
  validate_signatures: True
KSR-DOMAIN: Verified domain '.'
KSR-ID: Will be checked later, when SKR is available
KSR-BUNDLE-UNIQUE: All 9 bundles have unique ids
KSR-BUNDLE-KEYS: All 3 unique keys in the bundles accepted by policy
KSR-BUNDLE-POP: All 9 bundles contain proof-of-possession
KSR-BUNDLE-COUNT: Number of bundles (9) accepted
KSR-BUNDLE-CYCLE-DURATION: The cycle length is in accordance with the KSK operator policy
KSR-POLICY-KEYS: Validated number of keys per bundle, and for all bundles
KSR-POLICY-ALG: All 1 ZSK operator signature algorithms accepted by policy
KSR-POLICY-SIG-OVERLAP: All bundles overlap in accordance with the stated ZSK operator policy
KSR-POLICY-SIG-VALIDITY: All 9 bundles have 21 days <= validity >= 21 days
KSR-POLICY-SIG-HORIZON: All signatures expire in less than 180 days
KSR-POLICY-BUNDLE-INTERVALS: All bundles intervals in accordance with the KSK operator policy
Request:
#  Inception           Expiration          ZSK Tags      KSK(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  46780,11019
2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780
3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780
4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780
5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780
```

```
6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780
7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780
8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780
9  2023-12-20T00:00:00 2024-01-10T00:00:00  46780,30903
Initializing PKCS#11 module aep using /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86
_64.so.5.02
HSM First slot:      ICANNKSK
HSM ManufacturerID:  Ultra Electronics AEP Networks
HSM Model:           Keyper 9860-2
HSM Serial:          H1903017
Checking coherence between SKR(n-1) and this KSR
KSR-CHAIN-KEYS: The last keys in SKR(n-1) matches the first keys in this KSR
KSR-CHAIN-OVERLAP: Overlap with last bundle in SKR(n-1) 9 days is in accordance with the KSR policy
KSR-CHAIN-KEYS: All 1 signatures in the last bundle of the last SKR were made with keys present in th
e HSM(s)
KSR-POLICY-SAFETY: PublishSafety validated
KSR-POLICY-SAFETY: RetireSafety validated
Generated SKR:
#  Inception           Expiration          ZSK Tags      KSK(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  46780,11019   20326(Klajeyz)/S
2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780         20326(Klajeyz)/S
3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780         20326(Klajeyz)/S
4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780         20326(Klajeyz)/S
5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780         20326(Klajeyz)/S
6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780         20326(Klajeyz)/S
7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780         20326(Klajeyz)/S
8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780         20326(Klajeyz)/S
9  2023-12-20T00:00:00 2024-01-10T00:00:00  46780,30903   20326(Klajeyz)/S
Wrote SKR to file skr-root-2023-q4-0-new.xml SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a
9ff119e6cc5aed49 WORDS klaxon intention Neptune Virginia skullcap pharmacy ammo hesitate uproot getaw
ay retouch inventive trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getaw
ay unearth existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
```

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
24	CA deactivates the HSM by performing the following steps: **Note: CA will use OP cards not previously utilized in this ceremony if available.** a) CA selects the **HSM Output** terminal window. b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"2.Set Offline"**, press **ENT** to confirm. d) When **"Set Offline?"** is displayed, press **ENT** to confirm. e) When **"Insert Card OP #X?"** is displayed, insert the OP card from the card holder. f) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. g) When **"Remove Card?"** is displayed, remove the OP card. h) Repeat steps e) to g) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **OFF.** IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st OP card 6 of 7 2nd OP card 7 of 7 3rd OP card 1 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:00

OS Media Checksum Verification

Step	Activity	Initials	Time

25	CA uses the terminal window to executes the following steps:
	a) Verify the byte count of the SD card matches the **OS media release coen-1.0.0** ISO size of **375431168** by running the following command:
	`df -B1 /dev/sda`
	b) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sda | sha2wordlist`
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.
	
	SHA-256 hash:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note 1: The SHA-256 hash of the OS media is being calculated a second time to ensure the contents of the SD card have not been modified during the previous steps.
	Note 2: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/50
		Y.Y.	22:02

Act 5: Destroy OP and SO Cards

The Operator (OP) and Security Officer (SO) cards were originally issued in 2010 and have reached the end of their operational period. New OP and SO card sets were previously generated as replacements, and the original cards will now be destroyed.

The CA will destroy the OP and SO cards by performing the steps below:

- Clear the cards using an HSM's designated clear card function
- Slice through the cards' chips then place the cards in the shredder

Clear and Destroy OP and SO Cards

Step	Activity	Initials	Time
1	CA performs the following steps to clear Operator (OP) and Security Officer (SO) cards: a) CA selects the **HSM Output** terminal window. b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"7.Role Mgmt"**, press **ENT** to confirm. d) When **"Insert Card SO #X?"** is displayed, insert the SO card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the SO card. g) Repeat steps d) to f) for the 2nd and 3rd SO card. h) Select **"4.Clear RoleCard"**, press **ENT** to confirm. i) When **"Clear Card?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"9"**, then press **ENT**. k) When **"Insert Card #X?"** is displayed, take the required card, show the card to the audit camera and then insert the card into the HSM's card reader. l) When **"Are you sure?"** is displayed, press **ENT** to confirm. **Note: The message will differ depending of the card type.** m) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. n) When **"Remove Card?"** is displayed, remove the card. o) Repeat steps k) to n) until the specified cards have been cleared. p) Repeat steps h) to o) specifying **"6"** cards on step j). q) Press **CLR** to return to the main menu **"Secured"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st SO card 1 of 7 2nd SO card 2 of 7 3rd SO card 3 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:18
2	CA uses the shredder to destroy the cleared OP and SO cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.	Y.Y.	22:22

Act 6: KSK Import

The CA will import a new KSK by performing the steps below:

- Verify transported materials from the other KMF
- Set up and power on an HSM where the KSK is to be imported
- Use an App key backup card to import a KSK
- List and verify installed KSKs in the HSM
- Repeat previous steps for additional HSMs if necessary

Verify Transported Materials from the other KMF

Step	Activity	Initials	Time
1	CA performs the following steps to verify the transported materials from the other KMF: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **KSK-2023: TEB # BB02638527** ✓ Last Verified: KSK Ceremony 49 2023-04-27 / KSK Media Deposit 49 2023-04-29 **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.**	Y.Y.	22:24
2	CA plugs the **Ceremony 49 HSMFD** into the USB slot, then performs the steps below: a) Wait for the OS to recognize it as **HSMFD1** b) Display the HSMFD1 contents to all participants. c) Close the file system window.	Y.Y.	22:25

3	CA executes the command below using the **Commands** terminal window to calculate the SHA-256 hash of the HSMFD:
	
	`find -P /media/HSMFD1/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wordlist`
	
	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 2023/04/27
	`# find -P /media/HSMFD/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wordlist`
	`SHA-256: 1346fb2101014b50d6783f32b38df7b957adc00bb03857d5ad515ab66db1f2d2`
	`PGP Words: Aztec detergent watchword Camelot absurd adviser dragnet embezzle stockman indigo cowbell component scallion microscope virus proximate eightball perceptive slowdown armistice ruffled consulting eightball specialist ringbolt enchanting enlist potato goggles photograph uproot sensation`
	
	IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 49 annotated script.
		Y.Y.	22:27

Update Keymap File

Step	Activity	Initials	Time

4	CA performs the following steps using the terminal window to update the keymap file in the HSMFD:
	a) Copy the keymap file from HSMFD1 to HSMFD by executing:
	`cp -p /media/HSMFD1/KSKSlotDB.db .`
	Note: Confirm overwrite by entering "y"
	b) Verify it has been copied successfully by executing:
	`diff /media/HSMFD1/KSKSlotDB.db KSKSlotDB.db`
	c) Unmount the HSMFD1 by executing:
	`umount /media/HSMFD1`
	d) CA removes the **HSMFD1**, then place the equipment on its designated area of the ceremony table.
		Y.Y.	22:28

5	CA selects the **HSM Output** terminal window.	Y.Y.	22:28

Import the KSK

Step	Activity	Initials	Time
6	CA performs the following steps to access the Key Management menu: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd and 3rd CO card. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st CO card 1 of 7 2nd CO card 2 of 7 3rd CO card 3 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:30
7	CA performs the following steps to import KSK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required KSK card. g) When **"Remove Card?"** is displayed, remove the KSK card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR** to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. App Key card: **Copy # 1*** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:31
8	CA performs the following steps to list the App Keys from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. f) Press **CLR** to return to the main menu **"Secured"**.	Y.Y.	22:33
9	CA verifies the displayed KSK label in the **HSM Output** terminal window matches the imported key label. **KSK-2023 Label: Kmrfl3b**	Y.Y.	22:33

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
10	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.**	Y.Y.	22:33
11	CA places the HSM into its designated new TEB, then seals it.	Y.Y.	22:34
12	CA performs the following steps: a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM TEB on the cart. **HSM5W: TEB # BB51184282 ✓ / Serial # H1903017** ✓	Y.Y.	22:35

HSM (Tier 7) Setup

Step	Activity	Initials	Time
13	CA performs the following steps to prepare the HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM6W: TEB # BB51184545 ✓ / Serial # H2008009** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **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.**	Y.Y.	22:37

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM6W**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. **Note: Status information should appear in the HSM output logging screen.** d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H2008009**. ✓ e) Scroll down to the end of the logging screen. **HSM6W: Serial # H2008009** ✓ **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	Y.Y.	22:38

Import the KSK

Step	Activity	Initials	Time
15	CA performs the following steps to access the Key Management menu: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd and 3rd CO card. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st CO card 6 of 7 2nd CO card 7 of 7 3rd CO card 1 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:39
16	CA performs the following steps to import KSK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required KSK card. g) When **"Remove Card?"** is displayed, remove the KSK card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR** to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. App Key card: **Copy # 1*** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:40
17	CA performs the following steps to list the App Keys from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. f) Press **CLR** to return to the main menu **"Secured"**.	Y.Y.	22:41
18	CA verifies the displayed KSK label in the **HSM Output** terminal window matches the imported key label. **KSK-2023 Label: Kmrfl3b**	Y.Y.	22:41

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
19	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.**	Y.Y.	22:42
20	CA places the HSM into its designated new TEB, then seals it.	Y.Y.	22:42
21	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. **HSM6W: TEB # BB51184283 ✓ / Serial # H2008009** ✓	Y.Y.	22:43

HSM (Tier 7) Setup

Step	Activity	Initials	Time
22	CA performs the following steps to prepare the HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM7W: TEB # BB51184520 ✓ / Serial # H2110017** ✓ Last Verified: KSK Ceremony 48 2023-02-01 **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.**	Y.Y.	22:44

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
23	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM7W**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. **Note: Status information should appear in the HSM output logging screen.** d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H2110017**. e) Scroll down to the end of the logging screen. **HSM7W: Serial # H2110017** ✓ **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	Y.Y.	22:45

Import the KSK

Step	Activity	Initials	Time
24	CA performs the following steps to access the Key Management menu: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd and 3rd CO card. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st CO card 2 of 7 2nd CO card 3 of 7 3rd CO card 6 of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:47
25	CA performs the following steps to import KSK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required KSK card. g) When **"Remove Card?"** is displayed, remove the KSK card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR** to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. App Key card: **Copy # 2** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix A number [14].**	Y.Y.	22:48
26	CA performs the following steps to list the App Keys from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. f) Press **CLR** to return to the main menu **"Secured"**.	Y.Y.	22:48
27	CA verifies the displayed KSK label in the **HSM Output** terminal window matches the imported key label. **KSK-2023 Label: Kmrfl3b**	Y.Y.	22:48

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.**	Y.Y.	22~~:49~~
29	CA places the HSM into its designated new TEB, then seals it.	Y.Y.	22:49
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. **HSM7W: TEB # BB51184280 ✓ / Serial # H2110017** ✓	Y.Y.	22:50

Place the KSK Backups into a TEB

Step	Activity	Initials	Time
31	CA performs the following steps: a) CA places **KSK Backup Copy # 1*** and **KSK Backup Copy # 2**, and **2 Ceremony 49 HSMFDs** in a plastic case. b) CA places the plastic case and 1 sheet of paper with the printed **Ceremony 49 HSMFD hash** into its designated new TEB, then seals it.	Y.Y.	22:51
32	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number 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 TEB on the cart. **KSK-2023: TEB # BB02638507** ✓	Y.Y.	22:52

Act 7: Secure Hardware

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

- Copy 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 and COs into Tier 5 (Safe Room) to return COs' cards 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) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: i) Press `Ctrl + C` ii) Execute `exit` b) 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.** c) Disconnect the null modem and ethernet cables from the laptop.	Y.Y.	22:53

Print Logging Information

Step	Activity	Initials	Time
2	CA executes the following commands to print a copy of the logging information: a) `print-script script-202307*.log` b) `print-ttyaudit ttyaudit-tty*-202307*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**	Y.Y.	22:55

Prepare blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
3	CA executes the following command to print **two** copies of the hash for the HSMFD content: `hsmfd-hash -p` **Note: One copy for audit bundle and one copy for HSMFD package.**	Y.Y.	22:55
4	CA executes the command below to display the contents of the HSMFD: `ls -ltrR`	Y.Y.	22:55
5	CA executes the command below to create **five** HSMFDs copies: `copy-hsmfd` **Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.**	Y.Y.	23:02

HSMFD SHA-256 HASH **2023/07/19**

```
 # find -P /media/HSMFD/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wo
rdlist

 SHA-256:     6c50f24c1df087e5e37a1f4855053093b0e4ccb23299faaaa2c656fa89659332
PGP Words:  glucose embezzle uproot disbelief Belfast upcoming Neptune travesty tissue infa
ncy billiard dictator edict almighty chairlift molasses ruffled tradition spigot pioneer ch
eckup nebula wallet pedigree rebirth responsive egghead whimsical nightbird glossary playho
use component
```

```
Script started on 2023-07-19 21:21:41+00:00 [TERM="xterm-256color" TTY="/dev/pts/1" COLUMNS="101" LINES="33"]
\033[?2004h(kskm) 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=1.02 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.460 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.745 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.625 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3028ms
rtt min/avg/max/mdev = 0.460/0.711/1.016/0.202 ms
\033[?2004h(kskm) root@coen:/media/HSMFD# ksrsigner /media/KSRFD/KSK50/ksr-root-2023-q4-0.xml
Signing KSR with ksrsigner /media/KSRFD/KSK50/ksr-root-2023-q4-0.xml (at Wed Jul 19 21:47:50 2023 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:          H1903017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-07-01T00:00:00 2023-07-22T00:00:00  11019,60955   20326(Klajeyz)/S
2  2023-07-11T00:00:00 2023-08-01T00:00:00  11019         20326(Klajeyz)/S
3  2023-07-21T00:00:00 2023-08-11T00:00:00  11019         20326(Klajeyz)/S
4  2023-07-31T00:00:00 2023-08-21T00:00:00  11019         20326(Klajeyz)/S
5  2023-08-10T00:00:00 2023-08-31T00:00:00  11019         20326(Klajeyz)/S
6  2023-08-20T00:00:00 2023-09-10T00:00:00  11019         20326(Klajeyz)/S
7  2023-08-30T00:00:00 2023-09-20T00:00:00  11019         20326(Klajeyz)/S
8  2023-09-09T00:00:00 2023-09-30T00:00:00  11019         20326(Klajeyz)/S
9  2023-09-19T00:00:00 2023-10-10T00:00:00  46780,11019   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSRFD/KSK50/ksr-root-2023-q4-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  46780,11019
2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780
3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780
4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780
5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780
6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780
7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780
8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780
9  2023-12-20T00:00:00 2024-01-10T00:00:00  46780,30903
...PASSED.

SHA256 hash of KSR:
F139E2A852D76EE6C5E83C880C3308901358F87507F5E25CD79372C3142695C9
>> unwind corporate tiger paramount Dupont stethoscope goldfish trombonist solo typewriter cobra maritime ammo concurrent aimless millionaire Aztec everyday Vulcan impartial ahead visitor tiger fascinate stopwatch molasses highchair replica baboon caretaker preclude retrospect <<
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/KSRFD/KSK50/skr-root-2023-q4-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  46780,11019   20326(Klajeyz)/S
2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780         20326(Klajeyz)/S
3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780         20326(Klajeyz)/S
4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780         20326(Klajeyz)/S
5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780         20326(Klajeyz)/S
6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780         20326(Klajeyz)/S
7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780         20326(Klajeyz)/S
8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780         20326(Klajeyz)/S
9  2023-12-20T00:00:00 2024-01-10T00:00:00  30903,46780   20326(Klajeyz)/S

SHA256 hash of SKR:
4784544BD1E140A7DE787BD31B8DC884B269C63D8860401EBF91D63E2A7AB111
>> dashboard Jupiter eating disable stairway tolerance crackdown paragraph tactics indigo kickoff sociable beeswax microscope spaniel Jupiter sawdust guitarist southward crucifix newborn fortitude crackdown Burlington slingshot miracle stockman cumbersome brickyard infancy sailboat Babylon <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0

********** Log output in ./ksrsigner-20230719-214750.log **********
\033[?2004h(kskm) root@coen:/media/HSMFD# printlog ksr\007si\007gner-202307*.log 8
\033[?2004l11 copy ] sent to printer
2 lines were wrapped
\033[?2004h(kskm) root@coen:/media/HSMFD# cd /media/KSRFD/KSK50/new/
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK50/new# ksr\007k\007m\007-ksrsigner
2023-07-19 21:52:36,565: kskm.common.config: INFO Loaded configuration from file ksrsigner.yaml SHA-256 11e564d66bda046b76daac6311cf727391c13d06c41b5548864818eb1ea88be6 WORDS Athens travesty flytrap speculate glitter surrender adrift Hamilton inverse surrender ribcage Galveston Athens Saturday highchair hurricane pheasant recover commence amulet snowslide bravado edict dictator necklace dictator beaming underfoot berserk paramount obtuse trombonist
2023-07-19 21:52:36,606: kskm.common.config: INFO Configuration validated
2023-07-19 21:52:36,607: kskm.skr.load: INFO Loaded SKR from file skr-root-2023-q3-0.xml SHA-256 063f6815afbf4f3676a6b9fdea52d0a66c3706324639928c199ed5269d20468c5 WORDS afflict customer frighten bifocals rocker rebellion dropper congregate inverse paragon sentence Wyoming Trojan enrollment stagnate paragon glucose consensus afflict component cubic corporate breadline recover prowler unify Dupont guitarist standard alkali frighten resistor
2023-07-19 21:52:36,868: kskm.tools.ksrsigner: INFO Previous SKR:
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO #  Inception           Expiration          ZSK Tags      KSK(CKA_LABEL)
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 1  2023-07-01T00:00:00 2023-07-22T00:00:00  60955,11019   20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 2  2023-07-11T00:00:00 2023-08-01T00:00:00  11019         20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 3  2023-07-21T00:00:00 2023-08-11T00:00:00  11019         20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 4  2023-07-31T00:00:00 2023-08-21T00:00:00  11019         20326(Klajeyz)/S
```

```
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 5  2023-08-10T00:00:00 2023-08-31T00:
00:00  11019         20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 6  2023-08-20T00:00:00 2023-09-10T00:
00:00  11019         20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 7  2023-08-30T00:00:00 2023-09-20T00:
00:00  11019         20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 8  2023-09-09T00:00:00 2023-09-30T00:
00:00  11019         20326(Klajeyz)/S
2023-07-19 21:52:36,869: kskm.tools.ksrsigner: INFO 9  2023-09-19T00:00:00 2023-10-10T00:
00:00  46780,11019   20326(Klajeyz)/S
2023-07-19 21:52:36,870: kskm.ksr.load: INFO Loaded KSR from file ksr-root-2023-q4-0.xml
SHA-256 f139e2a852d76ee6c5e83c880c3308901358f87507f5e25cd79372c3142695c9 WORDS unwind cor
porate tiger paramount Dupont stethoscope goldfish trombonist solo typewriter cobra marit
ime ammo concurrent aimless millionaire Aztec everyday Vulcan impartial ahead visitor tig
er fascinate stopwatch molasses highchair replica baboon caretaker preclude retrospect
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO Validating KSR using request policy:
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   _dataclass_placeholder: None
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   acceptable_domains: ['.']
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   approved_algorithms: ['RSASHA256']
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   check_bundle_intervals: True
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   check_bundle_overlap: True
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   check_chain_keys: True
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   check_chain_keys_in_hsm: True
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   check_chain_overlap: True
2023-07-19 21:52:36,873: kskm.ksr.validate: INFO   check_cycle_length: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   check_keys_match_ksk_operator_policy:
True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   check_keys_publish_safety: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   check_keys_retire_safety: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   dns_ttl: 172800
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   enable_unsupported_ecdsa: False
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   keys_match_zsk_policy: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   max_bundle_interval: 11 days, 0:00:00
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   max_cycle_inception_length: 81 days, 0
:00:00
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   min_bundle_interval: 9 days, 0:00:00
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   min_cycle_inception_length: 79 days, 0
:00:00
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   num_bundles: 9
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   num_different_keys_in_all_bundles: 3
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   num_keys_per_bundle: [2, 1, 1, 1, 1, 1
, 1, 1, 2]
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   rsa_approved_exponents: [65537]
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   rsa_approved_key_sizes: [2048]
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   rsa_exponent_match_zsk_policy: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   signature_algorithms_match_zsk_policy:
 True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   signature_check_expire_horizon: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   signature_horizon_days: 180
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   signature_validity_match_zsk_policy: T
rue
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO   validate_signatures: True
2023-07-19 21:52:36,874: kskm.ksr.validate: INFO KSR-DOMAIN: Verified domain '.'
2023-07-19 21:52:36,875: kskm.ksr.validate: INFO KSR-ID: Will be checked later, when SKR
is available
2023-07-19 21:52:36,875: kskm.ksr.validate: INFO KSR-BUNDLE-UNIQUE: All 9 bundles have un
ique ids
2023-07-19 21:52:36,875: kskm.ksr.validate: INFO KSR-BUNDLE-KEYS: All 3 unique keys in th
e bundles accepted by policy
2023-07-19 21:52:36,876: kskm.ksr.validate: INFO KSR-BUNDLE-POP: All 9 bundles contain pr
oof-of-possession
2023-07-19 21:52:36,876: kskm.ksr.validate: INFO KSR-BUNDLE-COUNT: Number of bundles (9)
accepted
2023-07-19 21:52:36,876: kskm.ksr.validate: INFO KSR-BUNDLE-CYCLE-DURATION: The cycle len
gth is in accordance with the KSK operator policy
2023-07-19 21:52:36,876: kskm.ksr.validate: INFO KSR-POLICY-KEYS: Validated number of key
s per bundle, and for all bundles
2023-07-19 21:52:36,876: kskm.ksr.validate: INFO KSR-POLICY-ALG: All 1 ZSK operator signa
ture algorithms accepted by policy
2023-07-19 21:52:36,876: kskm.ksr.validate: INFO KSR-POLICY-SIG-OVERLAP: All bundles over
lap in accordance with the stated ZSK operator policy
2023-07-19 21:52:36,877: kskm.ksr.validate: INFO KSR-POLICY-SIG-VALIDITY: All 9 bundles h
ave 21 days <= validity >= 21 days
2023-07-19 21:52:36,877: kskm.ksr.validate: INFO KSR-POLICY-SIG-HORIZON: All signatures e
xpire in less than 180 days
2023-07-19 21:52:36,877: kskm.ksr.validate: INFO KSR-POLICY-BUNDLE-INTERVALS: All bundles
 intervals in accordance with the KSK operator policy
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO Request:
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO #  Inception           Expiration
      ZSK Tags      KSK(CKA_LABEL)
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 1  2023-10-01T00:00:00 2023-10-22T00:
00:00  46780,11019
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 2  2023-10-11T00:00:00 2023-11-01T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 3  2023-10-21T00:00:00 2023-11-11T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 4  2023-10-31T00:00:00 2023-11-21T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 5  2023-11-10T00:00:00 2023-12-01T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 6  2023-11-20T00:00:00 2023-12-11T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 7  2023-11-30T00:00:00 2023-12-21T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 8  2023-12-10T00:00:00 2023-12-31T00:
00:00  46780
2023-07-19 21:52:36,877: kskm.tools.ksrsigner: INFO 9  2023-12-20T00:00:00 2024-01-10T00:
00:00  46780,30903
2023-07-19 21:52:36,878: kskm.misc.hsm: INFO Initializing PKCS#11 module aep using /opt/K
eyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
2023-07-19 21:52:37,049: kskm.misc.hsm: INFO HSM First slot:       ICANNKSK

2023-07-19 21:52:37,050: kskm.misc.hsm: INFO HSM ManufacturerID:  Ultra Electronics AEP N
etworks
2023-07-19 21:52:37,050: kskm.misc.hsm: INFO HSM Model:           Keyper 9860-2
2023-07-19 21:52:37,050: kskm.misc.hsm: INFO HSM Serial:          H1903017
2023-07-19 21:52:37,050: kskm.signer.verify_chain: INFO Checking coherence between SKR(n-
1) and this KSR
2023-07-19 21:52:37,050: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: The last keys in
SKR(n-1) matches the first keys in this KSR
2023-07-19 21:52:37,051: kskm.signer.verify_chain: INFO KSR-CHAIN-OVERLAP: Overlap with l
ast bundle in SKR(n-1) 9 days is in accordance with the KSR policy
2023-07-19 21:52:37,051: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: All 1 signatures
in the last bundle of the last SKR were made with keys present in the HSM(s)

FILENAME:       ksr-root-2023-q4-0.xml
SHA-256 HEX:    f139e2a852d76ee6c5e83c880c3308901358f87507f5e25cd79372c3142695c9
SHA-256 WORDS:  unwind corporate tiger paramount Dupont stethoscope goldfish trombonist s
olo typewriter cobra maritime ammo concurrent aimless millionaire Aztec everyday Vulcan i
mpartial ahead visitor tiger fascinate stopwatch molasses highchair replica baboon careta
ker preclude retrospect

Sign KSR? Confirm with "Yes" (exactly) or anything else to abort: Yes
2023-07-19 21:53:35,059: kskm.signer.policy: INFO KSR-POLICY-SAFETY: PublishSafety valida
ted
2023-07-19 21:53:35,059: kskm.signer.policy: INFO KSR-POLICY-SAFETY: RetireSafety validat
ed
2023-07-19 21:53:35,059: kskm.tools.ksrsigner: INFO Generated SKR:
```

```
2023-07-19 21:53:35,059: kskm.tools.ksrsigner: INFO #  Inception           Expiration
      ZSK Tags      KSK(CKA_LABEL)
2023-07-19 21:53:35,059: kskm.tools.ksrsigner: INFO 1  2023-10-01T00:00:00 2023-10-22T00:
00:00  46780,11019   20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 2  2023-10-11T00:00:00 2023-11-01T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 3  2023-10-21T00:00:00 2023-11-11T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 4  2023-10-31T00:00:00 2023-11-21T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 5  2023-11-10T00:00:00 2023-12-01T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 6  2023-11-20T00:00:00 2023-12-11T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 7  2023-11-30T00:00:00 2023-12-21T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 8  2023-12-10T00:00:00 2023-12-31T00:
00:00  46780         20326(Klajeyz)/S
2023-07-19 21:53:35,060: kskm.tools.ksrsigner: INFO 9  2023-12-20T00:00:00 2024-01-10T00:
00:00  46780,30903   20326(Klajeyz)/S
2023-07-19 21:53:35,387: kskm.signer: INFO Wrote SKR to file skr-root-2023-q4-0-new.xml S
HA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9ff119e6cc5aed49 WORDS klaxon inte
ntion Neptune Virginia skullcap pharmacy ammo hesitate uproot getaway retouch inventive t
rouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getaway unearth
 existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK50/new# print\007log ksm\007\007\007\007\007
\007\007\007\007\007\007\007\007\007\007\007\007printlog kskm-ksrsigner-20230719-215236-990.l
og
\033[?2004l[ 1 copy ] sent to printer
6 lines were wrapped
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK50/new# xsltproc style.xsl ../sk\007r-root-20
23-q4-0.xml | xmllint --for
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK50/new# xsltproc style.xsl sk\007r-root-2023-
q4-0-new.xml | xmllint --fo
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK50/new# diff -wu current new
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK50/new# cd /media/HSMFD/
\033[?2004h(kskm) root@coen:/media/HSMFD# ls -ltrR /media/KSRFD/
/media/KSRFD/:
total 16
drwxr-xr-x 3 root root 16384 Jul 19 21:50 \033[0m\033[01;34mKSK50\033[0m

/media/KSRFD/KSK50:
total 160
-rw-r--r-- 1 root root 20369 Jul 12 20:10 skr.xml.20230719214750
-rw-r--r-- 1 root root 19600 Jul 12 20:10 ksr-root-2023-q4-0.xml
-rw-r--r-- 1 root root  1148 Jul 12 20:10 kskschedule.json
-rw-r--r-- 1 root root 20369 Jul 19 21:50 skr.xml
-rw-r--r-- 1 root root 20369 Jul 19 21:50 skr-root-2023-q4-0.xml
drwxr-xr-x 2 root root 16384 Jul 19 21:56 \033[01;34mnew\033[0m

/media/KSRFD/KSK50/new:
total 208
-rw-r--r-- 1 root root   652 Jul 12 20:10 style.xsl
-rw-r--r-- 1 root root 20369 Jul 12 20:10 skr-root-2023-q3-0.xml
-rw-r--r-- 1 root root 11505 Jul 12 20:10 ksrsigner.yaml
-rw-r--r-- 1 root root 19600 Jul 12 20:10 ksr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 24833 Jul 19 21:53 skr-root-2023-q4-0-new.xml
-rw-r--r-- 1 root root 11073 Jul 19 21:53 kskm-ksrsigner-20230719-215236-990.log
-rw-r--r-- 1 root root 22206 Jul 19 21:56 current
-rw-r--r-- 1 root root 22206 Jul 19 21:56 new
\033[?2004h(kskm) root@coen:/media/HSMFD# cp -pR /media/KSRFD/* .
\033[?2004h(kskm) root@coen:/media/HSMFD# ls -ltrR
\033[?2004l
total 3664
-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   9290 Feb  2  2012 ttyaudit-ttyUSB0-20120202-221813.log
-rw-r--r-- 1 root root  42056 Feb  2  2012 script-20120202.log
-rw-r--r-- 1 root root  18414 May 22  2012 skr.xml.20120726185458
-rw-r--r-- 1 root root  15391 Jul  3  2012 ksr-root-2012-q4-0.xml
-rw-r--r-- 1 root root  18324 Jul 26  2012 skr-root-2012-q4-0.xml
-rw-r--r-- 1 root root   5504 Jul 26  2012 ksrsigner-20120726-185458.log
-rw-r--r-- 1 root root  12034 Jul 26  2012 ttyaudit-ttyUSB0-20120726-184435.log
-rw-r--r-- 1 root root   5909 Jul 26  2012 script-20120726.log
-rw-r--r-- 1 root root  18314 Nov 12  2012 skr.xml.20130212222429
-rw-r--r-- 1 root root  15371 Jan 20  2013 ksr-root-2013-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 12  2013 skr-root-2013-q2-0.xml
-rw-r--r-- 1 root root   5506 Feb 12  2013 ksrsigner-20130212-222429.log
-rw-r--r-- 1 root root  12034 Feb 12  2013 ttyaudit-ttyUSB0-20130212-220521.log
-rw-r--r-- 1 root root   8385 Feb 12  2013 script-20130212.log
-rw-r--r-- 1 root root  18314 May  2  2013 skr.xml.20130807214313
-rw-r--r-- 1 root root  15371 Aug  5  2013 ksr-root-2013-q4-0.xml
-rw-r--r-- 1 root root  18314 Aug  7  2013 skr-root-2013-q4-0.xml
-rw-r--r-- 1 root root   5513 Aug  7  2013 ksrsigner-20130807-214313.log
-rw-r--r-- 1 root root   8192 Aug  7  2013 ttyaudit-ttyUSB0-20130807-213355.log
-rw-r--r-- 1 root root   5676 Aug  7  2013 script-20130807.log
-rw-r--r-- 1 root root  18314 Oct 24  2013 skr.xml.20140213225938
-rw-r--r-- 1 root root  15369 Jan 14  2014 ksr-root-2014-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 13  2014 skr-root-2014-q2-0.xml
-rw-r--r-- 1 root root   5513 Feb 13  2014 ksrsigner-20140213-225938.log
-rw-r--r-- 1 root root  12034 Feb 13  2014 ttyaudit-ttyUSB0-20140213-224635.log
```

```
-rw-r--r-- 1 root root   5638 Feb 13  2014 script-20140213.log
-rw-r--r-- 1 root root  18314 Apr 17  2014 skr.xml.20140814212827
-rw-r--r-- 1 root root  15369 Jul  7  2014 ksr-root-2014-q4-0.xml
-rw-r--r-- 1 root root      0 Aug 14  2014 ttyaudit-ttyUSB0-20140814-211101.log
-rw-r--r-- 1 root root  18314 Aug 14  2014 skr-root-2014-q4-0.xml
-rw-r--r-- 1 root root   5523 Aug 14  2014 ksrsigner-20140814-212827.log
-rw-r--r-- 1 root root  12032 Aug 14  2014 ttyaudit-ttyUSB0-20140814-211416.log
-rw-r--r-- 1 root root   5563 Aug 14  2014 script-20140814.log
-rw-r--r-- 1 root root  18314 Nov 20  2014 skr.xml.20150122223324
-rw-r--r-- 1 root root  15369 Jan 13  2015 ksr-root-2015-q2-0.xml
-rw-r--r-- 1 root root    762 Jan 13  2015 hash_ksr20.txt
-rw-r--r-- 1 root root  18314 Jan 22  2015 skr-root-2015-q2-0.xml
-rw-r--r-- 1 root root   5526 Jan 22  2015 ksrsigner-20150122-223324.log
-rw-r--r-- 1 root root  12034 Jan 22  2015 ttyaudit-ttyUSB0-20150122-222401.log
-rw-r--r-- 1 root root   5941 Jan 22  2015 script-20150122.log
-rw-r--r-- 1 root root  18314 Jul 28  2015 skr.xml.20150813213057
-rw-r--r-- 1 root root  15369 Jul 28  2015 ksr-root-2015-q4-0.xml
-rw-r--r-- 1 root root  18314 Aug 13  2015 skr-root-2015-q4-0.xml
-rw-r--r-- 1 root root   5505 Aug 13  2015 ksrsigner-20150813-213057.log
-rw-r--r-- 1 root root  17517 Aug 13  2015 ttyaudit-ttyUSB0-20150813-211033.log
-rw-r--r-- 1 root root   5520 Aug 13  2015 ksrsigner-20150814-000517.log
-rw-r--r-- 1 root root  43054 Aug 13  2015 ttyaudit-ttyUSB0-20150813-220137.log
-rw-r--r-- 1 root root   5520 Aug 13  2015 ksrsigner-20150814-002123.log
-rw-r--r-- 1 root root  44497 Aug 13  2015 ttyaudit-ttyUSB1-20150813-220137.log
-rw-r--r-- 1 root root  28755 Aug 13  2015 script-20150813.log
-rw-r--r-- 1 root root  18314 Jan 14  2016 skr.xml.20160211235227
-rw-r--r-- 1 root root  15371 Jan 14  2016 ksr-root-2016-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 11  2016 skr-root-2016-q2-0.xml
-rw-r--r-- 1 root root   5530 Feb 11  2016 ksrsigner-20160211-235227.log
-rw-r--r-- 1 root root  12196 Feb 11  2016 ttyaudit-ttyUSB0-20160211-234001.log
-rw-r--r-- 1 root root   6919 Feb 11  2016 script-20160211.log
-rw-r--r-- 1 root root  17908 May 12  2016 skr.xml.20160811220932
-rw-r--r-- 1 root root  14301 Jul 13  2016 ksr-root-2016-q4-fallback-1.xml
-rw-r--r-- 1 root root  21718 Jul 13  2016 ksr-root-2016-q4-0.xml
-rw-r--r-- 1 root root  18599 Jul 20  2016 skr.xml.20160811215735
-rw-r--r-- 1 root root  21083 Aug 11  2016 skr-root-2016-q4-0.xml
-rw-r--r-- 1 root root   5520 Aug 11  2016 ksrsigner-20160811-215735.log
-rw-r--r-- 1 root root  17908 Aug 11  2016 skr-root-2016-q4-fallback-1.xml
-rw-r--r-- 1 root root   5694 Aug 11  2016 ksrsigner-20160811-220932.log
-rw-r--r-- 1 root root  12499 Aug 11  2016 ttyaudit-ttyUSB0-20160811-213430.log
-rw-r--r-- 1 root root  33540 Aug 11  2016 ttyaudit-ttyUSB0-20160811-222510.log
-rw-r--r-- 1 root root  21200 Aug 11  2016 script-20160811.log
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr.xml.20170202225202
-rw-r--r-- 1 root root  19556 Jan  4  2017 ksr-root-2017-q2-0.xml
-rw-r--r-- 1 root root  20347 Feb  2  2017 skr.xml
-rw-r--r-- 1 root root  20347 Feb  2  2017 skr-root-2017-q2-0.xml
-rw-r--r-- 1 root root   5494 Feb  2  2017 ksrsigner-20170202-225202.log
-rw-r--r-- 1 root root    357 Feb  2  2017 keybackup-20170203-001846.log
-rw-r--r-- 1 root root   2693 Feb  2  2017 kskgen-20170203-001954.log
-rw-r--r-- 1 root root    817 Feb  2  2017 Klajeyz.csr
-rw-r--r-- 1 root root    357 Feb  2  2017 keybackup-20170203-003825.log
-rw-r--r-- 1 root root  48066 Feb  2  2017 ttyaudit-ttyUSB0-20170202-223524.log
-rw-r--r-- 1 root root  23999 Feb  2  2017 script-20170202.log
-rw-r--r-- 1 root root      0 Aug 17  2017 script-20170817.log
-rw-r--r-- 1 root root   8192 Aug 17  2017 ttyaudit-ttyUSB0-20170817-211909.log
-rw-r--r-- 1 root root   6645 Aug 17  2017 ksrsigner-20170817-214009.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[0m\033[01;34mKSK30-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6648 Aug 17  2017 ksrsigner-20170817-214402.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6662 Aug 17  2017 ksrsigner-20170817-214602.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6355 Aug 17  2017 ksrsigner-20170817-214756.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-3-C_to_C\033[0m
-rw-r--r-- 1 root root   2484 Aug 17  2017 ttyaudit-ttyUSB0-20170817-213501.log
-rw-r--r-- 1 root root  65904 Aug 17  2017 script-20170817-2.log
-rw-r--r-- 1 root root   6689 Feb  7  2018 ksrsigner-20180207-224219.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6676 Feb  7  2018 ksrsigner-20180207-224724.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6674 Feb  7  2018 ksrsigner-20180207-224920.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6367 Feb  7  2018 ksrsigner-20180207-225053.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-3-C_to_C\033[0m
-rw-r--r-- 1 root root  13737 Feb  7  2018 ttyaudit-ttyUSB0-20180207-222555.log
-rw-r--r-- 1 root root  23281 Feb  7  2018 script-20180207.log
-rw-r--r-- 1 root root   6774 Aug 15  2018 ksrsigner-20180815-221523.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6788 Aug 15  2018 ksrsigner-20180815-221858.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6798 Aug 15  2018 ksrsigner-20180815-222046.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6453 Aug 15  2018 ksrsigner-20180815-222210.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-3-C_to_C\033[0m
-rw-r--r-- 1 root root  14348 Aug 15  2018 ttyaudit-ttyS0-20180815-220248.log
-rw-r--r-- 1 root root  24749 Aug 15  2018 script-20180815.log
-rw-r--r-- 1 root root   6420 Feb 27  2019 ksrsigner-20190227-222718.log
drwxr-xr-x 2 root root   8192 Feb 27  2019 \033[01;34mKSK36\033[0m
-rw-r--r-- 1 root root  12372 Feb 27  2019 ttyaudit-ttyS0-20190227-221242.log
-rw-r--r-- 1 root root  22453 Feb 27  2019 script-20190227.log
-rw-r--r-- 1 root root   6252 Aug 14  2019 ksrsigner-20190814-215719.log
drwxr-xr-x 2 root root   8192 Aug 14  2019 \033[01;34mKSK38\033[0m
-rw-r--r-- 1 root root    357 Aug 14  2019 keybackup-20190814-231635.log
-rw-r--r-- 1 root root    210 Aug 14  2019 keybackup-20190814-231754.log
-rw-r--r-- 1 root root   1493 Aug 14  2019 KSKSlotDB.db
-rw-r--r-- 1 root root    271 Aug 14  2019 keybackup-20190814-231804.log
-rw-r--r-- 1 root root   6267 Aug 15  2019 ksrsigner-20190815-002322.log
-rw-r--r-- 1 root root  89867 Aug 15  2019 ttyaudit-ttyS0-20190814-213756.log
-rw-r--r-- 1 root root  29833 Aug 15  2019 script-20190814.log
-rw-r--r-- 1 root root   6280 Feb 16  2020 ksrsigner-20200216-022133.log
drwxr-xr-x 2 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
drwxr-xr-x 2 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
drwxr-xr-x 2 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
drwxr-xr-x 2 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
-rw-r--r-- 1 root root  36962 Apr 23  2020 script-20200423.log
-rw-r--r-- 1 root root   6295 Feb 11  2021 ksrsigner-20210211-191856.log
drwxr-xr-x 2 root root   8192 Feb 11  2021 \033[01;34mKSK42-2021-Q2\033[0m
-rw-r--r-- 1 root root   6958 Feb 11  2021 ksrsigner-20210211-192546.log
drwxr-xr-x 2 root root   8192 Feb 11  2021 \033[01;34mKSK42-2021-Q3\033[0m
-rw-r--r-- 1 root root   7169 Feb 11  2021 ksrsigner-20210211-192952.log
drwxr-xr-x 2 root root   8192 Feb 11  2021 \033[01;34mKSK42-2021-Q4\033[0m
-rw-r--r-- 1 root root  13763 Feb 11  2021 ttyaudit-ttyS0-20210211-190608.log
-rw-r--r-- 1 root root  38580 Feb 11  2021 script-20210211.log
-rw-r--r-- 1 root root   6248 Feb 16  2022 ksrsigner-20220216-224254.log
drwxr-xr-x 2 root root   8192 Feb 16  2022 \033[01;34mKSK44\033[0m
-rw-r--r-- 1 root root   6263 Feb 16  2022 ksrsigner-20220216-234715.log
-rw-r--r-- 1 root root  65325 Feb 17  2022 ttyaudit-ttyS0-20220216-222905.log
-rw-r--r-- 1 root root  34299 Feb 17  2022 script-20220216.log
drwxr-xr-x 2 root root   8192 Aug 17  2022 \033[01;34mKSK46\033[0m
-rw-r--r-- 1 root root   6251 Aug 17  2022 ksrsigner-20220817-211649.log
-rw-r--r-- 1 root root  85626 Aug 17  2022 ttyaudit-ttyS0-20220817-205940.log
-rw-r--r-- 1 root root  28220 Aug 17  2022 script-20220817.log
-rw-r--r-- 1 root root   6262 Feb  1 23:14 ksrsigner-20230201-231151.log
```

```
drwxr-xr-x 2 root root   8192 Feb  1 23:14 \033[01;34mKSK48\033[0m
-rw-r--r-- 1 root root   6277 Feb  2 00:38 ksrsigner-20230202-003711.log
-rw-r--r-- 1 root root  63923 Feb  2 00:47 ttyaudit-ttyS0-20230201-220329.log
-rw-r--r-- 1 root root  36701 Feb  2 00:58 script-20230201.log
drwxr-xr-x 2 root root   8192 Jul 19 21:50 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root   6280 Jul 19 21:50 ksrsigner-20230719-214750.log
drwxr-xr-x 3 root root   8192 Jul 19 21:50 \033[01;34mKSK50\033[0m
-rw-r--r-- 1 root root  14025 Jul 19 21:53 ttyaudit-ttyUSB0-20230719-212251.log
-rw-r--r-- 1 root root  16384 Jul 19 21:53 script-20230719.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
-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  2021 skr.xml.20210211191856
-rw-r--r-- 1 root root 19600 Feb  8  2021 ksr-root-2021-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb  8  2021 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11  2021 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11  2021 skr-root-2021-q2-0.xml

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

./KSK42-2021-Q4:
total 104
-rw-r--r-- 1 root root 19598 Feb  8  2021 ksr-root-2021-q4-0.xml
-rw-r--r-- 1 root root  1148 Feb  8  2021 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 11  2021 skr.xml.20210211192952
-rw-r--r-- 1 root root 20369 Feb 11  2021 skr.xml
-rw-r--r-- 1 root root 20369 Feb 11  2021 skr-root-2021-q4-0.xml

./KSK44:
total 104
-rw-r--r-- 1 root root 20369 Feb  2  2022 skr.xml.20220216224254
-rw-r--r-- 1 root root 19598 Feb  2  2022 ksr-root-2022-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb  2  2022 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16  2022 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16  2022 skr-root-2022-q2-0.xml

./KSK46:
total 104
-rw-r--r-- 1 root root 20369 Jul 11  2018 skr.xml.20220817211649
-rw-r--r-- 1 root root 19596 Jul 11  2018 ksr-root-2022-q4-0.xml
-rw-r--r-- 1 root root  1148 Jul 11  2018 kskschedule.json
-rw-r--r-- 1 root root 20369 Aug 17  2022 skr.xml
-rw-r--r-- 1 root root 20369 Aug 17  2022 skr-root-2022-q4-0.xml

./KSK48:
total 104
-rw-r--r-- 1 root root 20369 Jan 20 18:01 skr.xml.20230201231151
-rw-r--r-- 1 root root 19596 Jan 20 18:01 ksr-root-2023-q2-0.xml
-rw-r--r-- 1 root root  1148 Jan 20 18:01 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb  1 23:14 skr.xml
-rw-r--r-- 1 root root 20369 Feb  1 23:14 skr-root-2023-q2-0.xml

./tmp:
total 72
-rw-r--r-- 1 root root 1768 Jul 19 21:50 skr.keybundle.0
-rw-r--r-- 1 root root 1768 Jul 19 21:50 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.3
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Jul 19 21:50 skr.keybundle.1

./KSK50:
total 112
-rw-r--r-- 1 root root 20369 Jul 12 20:10 skr.xml.20230719214750
-rw-r--r-- 1 root root 19600 Jul 12 20:10 ksr-root-2023-q4-0.xml
-rw-r--r-- 1 root root  1148 Jul 12 20:10 kskschedule.json
-rw-r--r-- 1 root root 20369 Jul 19 21:50 skr.xml
-rw-r--r-- 1 root root 20369 Jul 19 21:50 skr-root-2023-q4-0.xml
drwxr-xr-x 2 root root  8192 Jul 19 21:56 \033[01;34mnew\033[0m

./KSK50/new:
total 168
-rw-r--r-- 1 root root   652 Jul 12 20:10 style.xsl
-rw-r--r-- 1 root root 20369 Jul 12 20:10 skr-root-2023-q3-0.xml
-rw-r--r-- 1 root root 11505 Jul 12 20:10 ksrsigner.yaml
-rw-r--r-- 1 root root 19600 Jul 12 20:10 ksr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 24833 Jul 19 21:53 skr-root-2023-q4-0-new.xml
-rw-r--r-- 1 root root 11073 Jul 19 21:53 kskm-ksrsigner-20230719-215236-990.log
-rw-r--r-- 1 root root 22206 Jul 19 21:56 current
-rw-r--r-- 1 root root 22206 Jul 19 21:56 new
\033[?2004h(kskm) root@coen:/media/HSMFD# diff -qr /media/HSMFD/K\007h\007S\007K50/ /m\007
edia/\007KSRFD/KSK50/
\033[?2004h(kskm) root@coen:/media/HSMFD# umount /media/KSRFD/
\033[?2004h(kskm) root@coen:/media/HSMFD# df -B1 /dev/sda
Filesystem     1B-blocks      Used Available Use% Mounted on
/dev/sda       375431168 375431168         0 100% /run/live/medium
\033[?2004h(kskm) root@coen:/media/HSMFD# head -c \033[7m375431168\033[27m /dev/sda | sha
2wordlist
SHA256 405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
PGP Words:  crackdown filament kiwi impetus snapline belowground woodlark proximate cowbe
ll revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead ch
oking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eatin
g autopsy snapline corrosion
\033[?2004h(kskm) root@coen:/media/HSMFD# find -P /media/HS\007MFD1/ -type f -print0 | LC
SHA256 1346fb2101014b50d6783f32b38df7b957adc00bb03857d5ad515ab66db1f2d2
PGP Words:  Aztec detergent watchword Camelot absurd adviser dragnet embezzle stockman in
digo cowbell component scallion microscope virus proximate eightball perceptive slowdown
armistice ruffled consulting eightball specialist ringbolt enchanting enlist potato goggl
es photograph uproot sensation
\033[?2004h(kskm) root@coen:/media/HSMFD# cp -P /m\007edia/HS\007MFD1/KS\007KSl\007otDB.d
b .
\033[?2004h(kskm) root@coen:/media/HSMFD# pdd
```

```
X[illegible]
\033[?2004h(kskm) root@coen:/media/HSMFD# diff /media/HS\007MFD1/KS\007KS\007lotDB.db KS
\007KS\007lotDB.db
\033[?2004h(kskm) root@coen:/media/HSMFD# um\007o\007unt /m\007edia/HS\007MFD1/
\033[?2004h(kskm) root@coen:/media/HSMFD#
\033[?2004l

Script done on 2023-07-19 22:52:49+00:00 [COMMAND_EXIT_CODE="0"]
```

```
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 H1903017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 H1903017 011403 ABL 030 : Tamper Challenge Response Key
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ####################################
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ###     ABL tamper records       ###
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ####################################
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ====================================
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 vextoosTamperCount:     0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 vintoosTamperCount:     8
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 vbboosTamperCount:      0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 minstrtempTamperCount:  0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 meshTamperCount:        0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 extampSMKTamperCount:   0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 extampIMKTamperCount:   0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 tempdiffTamperCount:    0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 pfTamperCount:          8
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 restartTamperCount:     24
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 Current tamper bitmaps:
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ======================
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0 ============================================
2023-07-19T21:24:03+0000        ttyUSB0
```

```
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:03+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0 Board is P2020RDB
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0 board_smp_init: 2 cpu
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:05+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-07-19T21:24:05+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 Starting next program at v0015183c
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 Starting K-Series Kernel
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 Fri Apr  5 06:07:39 1974
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 Starting auditd v2.0 ... started.
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:06+0000        ttyUSB0 Interface 0 configured for IPv6.
2023-07-19T21:24:06+0000        ttyUSB0
2023-07-19T21:24:07+0000        ttyUSB0 Interface 0 configured for IPv4.
2023-07-19T21:24:07+0000        ttyUSB0
2023-07-19T21:24:07+0000        ttyUSB0 Interface 1 configured for IPv6.
2023-07-19T21:24:07+0000        ttyUSB0
2023-07-19T21:24:07+0000        ttyUSB0 Interface 1 configured for IPv4.
2023-07-19T21:24:07+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0 Starting USB driver...
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:08+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running DES POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 DES POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running Triple DES POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Triple DES POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running AES POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 AES POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
```

```
2023-07-19T21:24:09+0000        ttyUSB0 Running SHA1 POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 SHA1 POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running SHA2 POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 SHA2 POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running RandomGen POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 RandomGen POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running RSA POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 RSA POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running DSA POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 DSA POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running SEED POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 SEED POST Test Passed
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:09+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-07-19T21:24:09+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 Running ECC POST Test
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 ECC POST Test Passed
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 Running HMAC POST Tests
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 HMAC POST Tests Passed
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 Audit on 5/4/1974 06:07:42 00100008
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 Keyper 9860-2  Serial Number H1903017
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:10+0000        ttyUSB0 Memory Usage:
2023-07-19T21:24:10+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0    black store          524b
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0    statistics           112b
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0    other                116b
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
```

```
2023-07-19T21:24:11+0000        ttyUSB0 Network Configuration:
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 Interface 0:
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0     IPv4: enabled
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0     IPv6: enabled
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C4:9A / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c49a/64
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 Interface 1:
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0     IPv4: enabled
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0     IPv6: enabled
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C4:9B / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c49b/64
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 HSM Port 0: 05000
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 HSM Port 1: 03000
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 Software Versions:
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 CPLD Version:
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 1.9
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 SCR Firmware Version:
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 OROS-R2.99-R1.20
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 HmcListener: Created IPv4 socket 12 on port 3000.
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 HmcListener: Created IPv6 socket 13 on port 3000.
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:24:11+0000        ttyUSB0 Audit on 5/4/1974 06:07:44 00100003
2023-07-19T21:24:11+0000        ttyUSB0
2023-07-19T21:44:03+0000        ttyUSB0 Audit on 5/4/1974 06:27:35 00200069 3F400032D64A2A77
2023-07-19T21:44:03+0000        ttyUSB0
2023-07-19T21:44:20+0000        ttyUSB0 Audit on 5/4/1974 06:27:53 0020006a
2023-07-19T21:44:20+0000        ttyUSB0
2023-07-19T21:44:43+0000        ttyUSB0 Audit on 5/4/1974 06:28:16 00200069 3F400032D70A2A77
2023-07-19T21:44:43+0000        ttyUSB0
2023-07-19T21:45:04+0000        ttyUSB0 Audit on 5/4/1974 06:28:36 00200069 3F400031D48A2A77
2023-07-19T21:45:04+0000        ttyUSB0
2023-07-19T21:45:06+0000        ttyUSB0
2023-07-19T21:45:06+0000        ttyUSB0
```

```
2023-07-19T21:45:06+0000        ttyUSB0 TcpListener: Created IPv4 socket 19 on port 5000.
2023-07-19T21:45:06+0000        ttyUSB0
2023-07-19T21:45:06+0000        ttyUSB0
2023-07-19T21:45:06+0000        ttyUSB0
2023-07-19T21:45:06+0000        ttyUSB0 TcpListener: Created IPv6 socket 20 on port 5000.
2023-07-19T21:45:06+0000        ttyUSB0
2023-07-19T21:45:06+0000        ttyUSB0 Audit on 5/4/1974 06:28:38 00100002
2023-07-19T21:45:06+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0 TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0 CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:47:59+0000        ttyUSB0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2023-07-19T21:47:59+0000        ttyUSB0
2023-07-19T21:50:21+0000        ttyUSB0
2023-07-19T21:50:21+0000        ttyUSB0
2023-07-19T21:50:21+0000        ttyUSB0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2023-07-19T21:50:21+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0 TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0 CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:52:36+0000        ttyUSB0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2023-07-19T21:52:36+0000        ttyUSB0
2023-07-19T21:53:35+0000        ttyUSB0
2023-07-19T21:53:35+0000        ttyUSB0
2023-07-19T21:53:35+0000        ttyUSB0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2023-07-19T21:53:35+0000        ttyUSB0
2023-07-19T21:59:56+0000        ttyUSB0 Audit on 5/4/1974 06:43:28 00200069 3F4000339F4A2A77
2023-07-19T21:59:56+0000        ttyUSB0
2023-07-19T22:00:16+0000        ttyUSB0 Audit on 5/4/1974 06:43:48 00200069 3F4000339ECA2A77
2023-07-19T22:00:16+0000        ttyUSB0
2023-07-19T22:00:34+0000        ttyUSB0 Audit on 5/4/1974 06:44:07 00200069 3F400032D64A2A77
2023-07-19T22:00:34+0000        ttyUSB0
2023-07-19T22:00:36+0000        ttyUSB0
2023-07-19T22:00:36+0000        ttyUSB0
2023-07-19T22:00:36+0000        ttyUSB0 TcpListener: Closed IPv4 socket 19 on port 5000.
2023-07-19T22:00:36+0000        ttyUSB0
2023-07-19T22:00:36+0000        ttyUSB0
2023-07-19T22:00:36+0000        ttyUSB0
2023-07-19T22:00:36+0000        ttyUSB0 TcpListener: Closed IPv6 socket 20 on port 5000.
2023-07-19T22:00:36+0000        ttyUSB0
2023-07-19T22:00:37+0000        ttyUSB0 Audit on 5/4/1974 06:44:09 00100003
2023-07-19T22:00:37+0000        ttyUSB0
2023-07-19T22:02:49+0000        ttyUSB0 Audit on 5/4/1974 06:46:22 00200023 3F400031D50A2A77
2023-07-19T22:02:49+0000        ttyUSB0
2023-07-19T22:03:12+0000        ttyUSB0 Audit on 5/4/1974 06:46:44 00200023 3F400031D58A2A77
2023-07-19T22:03:12+0000        ttyUSB0
2023-07-19T22:03:36+0000        ttyUSB0 Audit on 5/4/1974 06:47:08 00200023 3F400031CF4A2A77
2023-07-19T22:03:36+0000        ttyUSB0
2023-07-19T22:05:27+0000        ttyUSB0 Audit on 5/4/1974 06:49:00 0020002f 0A400000BA06296E
2023-07-19T22:05:27+0000        ttyUSB0
```

```
2023-07-19T22:06:24+0000        ttyUSB0 Audit on 5/4/1974 06:49:57 0020002f 0A400000B786296E
2023-07-19T22:06:24+0000        ttyUSB0
2023-07-19T22:07:13+0000        ttyUSB0 Audit on 5/4/1974 06:50:45 0020006f 0A4000009DC6296E
2023-07-19T22:07:13+0000        ttyUSB0
2023-07-19T22:08:42+0000        ttyUSB0 Audit on 5/4/1974 06:52:15 0020006f 0A400000B7C6296E
2023-07-19T22:08:42+0000        ttyUSB0
2023-07-19T22:09:33+0000        ttyUSB0 Audit on 5/4/1974 06:53:06 0020002f 0A400000B846296E
2023-07-19T22:09:33+0000        ttyUSB0
2023-07-19T22:10:19+0000        ttyUSB0 Audit on 5/4/1974 06:53:51 0020002f 0A400000BAC6296E
2023-07-19T22:10:19+0000        ttyUSB0
2023-07-19T22:11:12+0000        ttyUSB0 Audit on 5/4/1974 06:54:45 0020002f 0A400000BA46296E
2023-07-19T22:11:12+0000        ttyUSB0
2023-07-19T22:11:56+0000        ttyUSB0 Audit on 5/4/1974 06:55:29 0020002f 0A400000B886296E
2023-07-19T22:11:56+0000        ttyUSB0
2023-07-19T22:12:39+0000        ttyUSB0 Audit on 5/4/1974 06:56:11 0020006f 0A400000B646296E
2023-07-19T22:12:39+0000        ttyUSB0
2023-07-19T22:14:10+0000        ttyUSB0 Audit on 5/4/1974 06:57:43 0020006f 0A400000B706296E
2023-07-19T22:14:10+0000        ttyUSB0
2023-07-19T22:14:59+0000        ttyUSB0 Audit on 5/4/1974 06:58:31 0020002f 0A400000B946296E
2023-07-19T22:14:59+0000        ttyUSB0
2023-07-19T22:15:42+0000        ttyUSB0 Audit on 5/4/1974 06:59:14 0020002f 0A400000DB46296E
2023-07-19T22:15:42+0000        ttyUSB0
2023-07-19T22:16:31+0000        ttyUSB0 Audit on 5/4/1974 07:00:03 0020002f 0A400000DB06296E
2023-07-19T22:16:31+0000        ttyUSB0
2023-07-19T22:17:13+0000        ttyUSB0 Audit on 5/4/1974 07:00:45 0020002f 0A400000B906296E
2023-07-19T22:17:13+0000        ttyUSB0
2023-07-19T22:17:56+0000        ttyUSB0 Audit on 5/4/1974 07:01:29 0020006f 0A4000009D06296E
2023-07-19T22:17:56+0000        ttyUSB0
2023-07-19T22:29:05+0000        ttyUSB0 Audit on 5/4/1974 07:12:37 0020006c
2023-07-19T22:29:05+0000        ttyUSB0
2023-07-19T22:29:24+0000        ttyUSB0 Audit on 5/4/1974 07:12:56 0020006b 398001161DA72A76
2023-07-19T22:29:24+0000        ttyUSB0
2023-07-19T22:29:44+0000        ttyUSB0 Audit on 5/4/1974 07:13:17 0020006b 398001161EA72A76
2023-07-19T22:29:44+0000        ttyUSB0
2023-07-19T22:30:05+0000        ttyUSB0 Audit on 5/4/1974 07:13:38 0020006b 39800115FA272A76
2023-07-19T22:30:05+0000        ttyUSB0
2023-07-19T22:31:34+0000        ttyUSB0 Audit on 5/4/1974 07:15:06 00200016 Kmrfl3b
2023-07-19T22:31:34+0000        ttyUSB0
2023-07-19T22:31:34+0000        ttyUSB0 Audit on 5/4/1974 07:15:06 00200015 3F400031F94A2A77
2023-07-19T22:31:34+0000        ttyUSB0
2023-07-19T22:31:34+0000        ttyUSB0 Audit on 5/4/1974 07:15:06 00200018
2023-07-19T22:31:34+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0 ================================================
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0 Key Details
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0 ================================================
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0 Klajeyz,RSA,FIPS,2048,wt,svedmvu
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0 Kmrfl3b,RSA,FIPS,2048,wt,sd
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0 ================================================
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:08+0000        ttyUSB0
2023-07-19T22:32:21+0000        ttyUSB0
2023-07-19T22:32:21+0000        ttyUSB0
2023-07-19T22:32:22+0000        ttyUSB0 ================================================
2023-07-19T22:32:22+0000        ttyUSB0
2023-07-19T22:32:22+0000        ttyUSB0 Key Summary
2023-07-19T22:32:22+0000        ttyUSB0
```

```
2023-07-19T22:32:22+0000        ttyUSB0 ------------------------------------------------------------
2023-07-19T22:32:22+0000        ttyUSB0
2023-07-19T22:32:22+0000        ttyUSB0 RSA,2048,Private,2
2023-07-19T22:32:22+0000        ttyUSB0
2023-07-19T22:32:22+0000        ttyUSB0 ------------------------------------------------------------
2023-07-19T22:32:22+0000        ttyUSB0
2023-07-19T22:32:22+0000        ttyUSB0
2023-07-19T22:32:22+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 H2008009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 H2008009 011403 ABL 030 : Tamper Challenge Response Key
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 ####################################
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 ###     ABL tamper records       ###
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 ####################################
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 ------------------------------------------------------------
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 vextoosTamperCount:     0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 vintoosTamperCount:     5
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 vbboosTamperCount:      0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 minstrtempTamperCount:  0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 meshTamperCount:        0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 extampSMKTamperCount:   0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 extampIMKTamperCount:   0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 tempdiffTamperCount:    0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 pfTamperCount:          5
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 restartTamperCount:     14
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 Current tamper bitmaps:
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 ------------------------------
2023-07-19T22:37:50+0000        ttyUSB0
2023-07-19T22:37:50+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-07-19T22:37:50+0000        ttyUSB0
```

```
2023-07-19T22:37:50+0000     ttyUSB0 lastTamper bitmap:     0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:50+0000     ttyUSB0 Bitmapped Change Record (most recent first):
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:50+0000     ttyUSB0 ------------------------------------------------------------
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:50+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0 Jumping to startup @ 0x001037B4
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0 Board is P2020RDB
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0 board_smp_init: 2 cpu
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:52+0000     ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-07-19T22:37:52+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0 Starting next program at v0015183c
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0 Starting K-Series Kernel
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0 Sat Oct 16 13:33:49 1971
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:53+0000     ttyUSB0 Starting auditd v2.0 ... started.
2023-07-19T22:37:53+0000     ttyUSB0
2023-07-19T22:37:54+0000     ttyUSB0 Interface 0 configured for IPv6.
2023-07-19T22:37:54+0000     ttyUSB0
2023-07-19T22:37:54+0000     ttyUSB0 Interface 0 configured for IPv4.
2023-07-19T22:37:54+0000     ttyUSB0
2023-07-19T22:37:54+0000     ttyUSB0 Interface 1 configured for IPv6.
2023-07-19T22:37:54+0000     ttyUSB0
2023-07-19T22:37:54+0000     ttyUSB0 Interface 1 configured for IPv4.
2023-07-19T22:37:54+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0 route: writing to routing socket: Network is unreachable
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0 add net default: gateway ::: Network is unreachable
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0 route: writing to routing socket: Network is unreachable
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0 Starting USB driver...
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:55+0000     ttyUSB0
2023-07-19T22:37:56+0000     ttyUSB0
2023-07-19T22:37:56+0000     ttyUSB0
2023-07-19T22:37:56+0000     ttyUSB0 Running DES POST Test
2023-07-19T22:37:56+0000     ttyUSB0
2023-07-19T22:37:56+0000     ttyUSB0 DES POST Test Passed
2023-07-19T22:37:56+0000     ttyUSB0
```

```
2023-07-19T22:37:57+0000        ttyUSB0 Running Triple DES POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Triple DES POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running AES POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 AES POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running SHA1 POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 SHA1 POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running SHA2 POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 SHA2 POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running RandomGen POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 RandomGen POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running RSA POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 RSA POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running DSA POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 DSA POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running SEED POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 SEED POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running ECC POST Test
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 ECC POST Test Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Running HMAC POST Tests
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 HMAC POST Tests Passed
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0 Audit on 16/10/1971 13:33:52 00100008
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:57+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Keyper 9860-2  Serial Number H2008009
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Memory Usage:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0    black store          524b
2023-07-19T22:37:58+0000        ttyUSB0
```

```
2023-07-19T22:37:58+0000        ttyUSB0    statistics           112b
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0    other                116b
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Network Configuration:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Interface 0:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0     IPv4: enabled
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0     IPv6: enabled
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C8:52 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c852/64
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Interface 1:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0     IPv4: enabled
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0     IPv6: enabled
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C8:53 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c853/64
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 HSM Port 0: 05000
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 HSM Port 1: 03000
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Software Versions:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 CPLD Version:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 1.9
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 SCR Firmware Version:
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 OROS-R2.99-R1.20
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 HmcListener: Created IPv4 socket 12 on port 3000.
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 HmcListener: Created IPv6 socket 13 on port 3000.
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:37:58+0000        ttyUSB0 Audit on 16/10/1971 13:33:53 00100003
2023-07-19T22:37:58+0000        ttyUSB0
2023-07-19T22:39:00+0000        ttyUSB0 Audit on 16/10/1971 13:34:55 0020006b 398001160E272A76
2023-07-19T22:39:00+0000        ttyUSB0
```

```
2023-07-19T22:39:23+0000        ttyUSB0 Audit on 16/10/1971 13:35:19 0020006b 39800115FDA72A76
2023-07-19T22:39:23+0000        ttyUSB0
2023-07-19T22:39:46+0000        ttyUSB0 Audit on 16/10/1971 13:35:41 0020006b 398001161DA72A76
2023-07-19T22:39:46+0000        ttyUSB0
2023-07-19T22:40:31+0000        ttyUSB0 Audit on 16/10/1971 13:36:27 00200016 Kmrfl3b
2023-07-19T22:40:31+0000        ttyUSB0
2023-07-19T22:40:31+0000        ttyUSB0 Audit on 16/10/1971 13:36:27 00200015 3F400031F94A2A77
2023-07-19T22:40:31+0000        ttyUSB0
2023-07-19T22:40:31+0000        ttyUSB0 Audit on 16/10/1971 13:36:27 00200018
2023-07-19T22:40:31+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0 ================================================
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0 Key Details
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0 ================================================
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0 Klajeyz,RSA,FIPS,2048,wt,svedmvu
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0 Kmrfl3b,RSA,FIPS,2048,wt,sd
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0 ================================================
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:02+0000        ttyUSB0
2023-07-19T22:41:06+0000        ttyUSB0
2023-07-19T22:41:06+0000        ttyUSB0
2023-07-19T22:41:06+0000        ttyUSB0 ================================================
2023-07-19T22:41:06+0000        ttyUSB0
2023-07-19T22:41:07+0000        ttyUSB0 Key Summary
2023-07-19T22:41:07+0000        ttyUSB0
2023-07-19T22:41:07+0000        ttyUSB0 ================================================
2023-07-19T22:41:07+0000        ttyUSB0
2023-07-19T22:41:07+0000        ttyUSB0 RSA,2048,Private,2
2023-07-19T22:41:07+0000        ttyUSB0
2023-07-19T22:41:07+0000        ttyUSB0 ================================================
2023-07-19T22:41:07+0000        ttyUSB0
2023-07-19T22:41:07+0000        ttyUSB0
2023-07-19T22:41:07+0000        ttyUSB0
2023-07-19T22:45:30+0000        ttyUSB0
2023-07-19T22:45:30+0000        ttyUSB0
2023-07-19T22:45:30+0000        ttyUSB0 H2110017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-07-19T22:45:30+0000        ttyUSB0
2023-07-19T22:45:30+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-07-19T22:45:30+0000        ttyUSB0
2023-07-19T22:45:30+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-07-19T22:45:30+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 H2110017 011403 ABL 030 : Tamper Challenge Response Key
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 ####################################
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 ###     ABL tamper records       ###
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 ####################################
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-07-19T22:45:31+0000        ttyUSB0
```

```
2023-07-19T22:45:31+0000        ttyUSB0 ========================================
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 vextoosTamperCount:     0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 vintoosTamperCount:     5
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 vbboosTamperCount:      0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 minstrtempTamperCount:  0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 meshTamperCount:        0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 extampSMKTamperCount:   0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 extampIMKTamperCount:   0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 tempdiffTamperCount:    0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 pfTamperCount:          5
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 restartTamperCount:     12
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 Current tamper bitmaps:
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 ========================
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0 ========================================
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:31+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0 Board is P2020RDB
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0 board_smp_init: 2 cpu
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:32+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-07-19T22:45:32+0000        ttyUSB0
2023-07-19T22:45:33+0000        ttyUSB0
2023-07-19T22:45:33+0000        ttyUSB0
2023-07-19T22:45:33+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-07-19T22:45:33+0000        ttyUSB0
2023-07-19T22:45:33+0000        ttyUSB0 Starting next program at v0015183c
2023-07-19T22:45:33+0000        ttyUSB0
2023-07-19T22:45:33+0000        ttyUSB0 Starting K-Series Kernel
2023-07-19T22:45:33+0000        ttyUSB0
2023-07-19T22:45:33+0000        ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-07-19T22:45:33+0000        ttyUSB0
```

```
2023-07-19T22:45:33+0000        ttyUSB0 Sat Jul 11 13:21:16 1970
2023-07-19T22:45:33+0000        ttyUSB0
2023-07-19T22:45:34+0000        ttyUSB0 Starting auditd v2.0 ... started.
2023-07-19T22:45:34+0000        ttyUSB0
2023-07-19T22:45:34+0000        ttyUSB0 Interface 0 configured for IPv6.
2023-07-19T22:45:34+0000        ttyUSB0
2023-07-19T22:45:34+0000        ttyUSB0 Interface 0 configured for IPv4.
2023-07-19T22:45:34+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 Interface 1 configured for IPv6.
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 Interface 1 configured for IPv4.
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 Starting USB driver...
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:35+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running DES POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 DES POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running Triple DES POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Triple DES POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running AES POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 AES POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running SHA1 POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 SHA1 POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running SHA2 POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 SHA2 POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running RandomGen POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 RandomGen POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running RSA POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 RSA POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running DSA POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 DSA POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running SEED POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 SEED POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
```

```
2023-07-19T22:45:37+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running ECC POST Test
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 ECC POST Test Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 Running HMAC POST Tests
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:37+0000        ttyUSB0 HMAC POST Tests Passed
2023-07-19T22:45:37+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Audit on 11/7/1970 13:21:19 00100008
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Keyper 9860-2  Serial Number H2110017
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Memory Usage:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0    black store          524b
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0    statistics           112b
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0    other                116b
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Network Configuration:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Interface 0:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0     IPv4: enabled
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0     IPv6: enabled
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:66 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c966/64
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Interface 1:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0     IPv4: enabled
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0     IPv6: enabled
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:67 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c967/64
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 HSM Port 0: 05000
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 HSM Port 1: 03000
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-07-19T22:45:38+0000        ttyUSB0
```

```
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Software Versions:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 CPLD Version:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 1.9
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 SCR Firmware Version:
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 OROS-R2.99-R1.20
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 HmcListener: Created IPv4 socket 12 on port 3000.
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 HmcListener: Created IPv6 socket 13 on port 3000.
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:45:38+0000        ttyUSB0 Audit on 11/7/1970 13:21:20 00100003
2023-07-19T22:45:38+0000        ttyUSB0
2023-07-19T22:46:24+0000        ttyUSB0 Audit on 11/7/1970 13:22:06 0020006b 398001161EA72A76
2023-07-19T22:46:24+0000        ttyUSB0
2023-07-19T22:46:44+0000        ttyUSB0 Audit on 11/7/1970 13:22:26 0020006b 39800115FA272A76
2023-07-19T22:46:44+0000        ttyUSB0
2023-07-19T22:47:06+0000        ttyUSB0 Audit on 11/7/1970 13:22:48 0020006b 398001160E272A76
2023-07-19T22:47:06+0000        ttyUSB0
2023-07-19T22:47:56+0000        ttyUSB0 Audit on 11/7/1970 13:23:38 00200016 Kmrfl3b
2023-07-19T22:47:56+0000        ttyUSB0
2023-07-19T22:47:57+0000        ttyUSB0 Audit on 11/7/1970 13:23:38 00200015 3F400031F90A2A77
2023-07-19T22:47:57+0000        ttyUSB0
2023-07-19T22:47:57+0000        ttyUSB0 Audit on 11/7/1970 13:23:39 00200018
2023-07-19T22:47:57+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0 ==========
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0 Key Details
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0 ==========
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0 Klajeyz,RSA,FIPS,2048,wt,svedmvu
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0 Kmrfl3b,RSA,FIPS,2048,wt,sd
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0 ==========
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:11+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0 ==========
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0 Key Summary
2023-07-19T22:48:13+0000        ttyUSB0
```

```
2023-07-19T22:48:13+0000        ttyUSB0 ==========
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0 RSA,2048,Private,2
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0 ==========
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0
2023-07-19T22:48:13+0000        ttyUSB0
```

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
6	CA executes the following commands using the terminal window to unmount the HSMFD: a) `cd /tmp` b) `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder. **Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.**	Y.Y.	23:04
7	CA performs the following steps to switch OFF the laptop and remove the OS media: a) Turn OFF the laptop by pressing the power button. b) Disconnect all connections from the laptop. c) Remove the OS media from the laptop.	Y.Y.	23:05
8	CA places 2 HSMFDs, 2 OS media SD cards enclosed in their plastic cases, 2 OS media DVDs, and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seals it.	Y.Y.	23:06
9	CA performs the following steps to verify the TEB: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS media TEB on the cart. **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638508** ✓	Y.Y.	23:07
10	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	Y.Y.	23:07

Place the Laptop into a TEB

Step	Activity	Initials	Time
11	CA places the laptop into its designated new TEB, then seals it.	Y.Y.	23:08
12	CA performs the following steps: a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and laptop serial number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the laptop TEB on the cart. **Laptop4: TEB # BB81420076** ✓ **/ Service Tag # F8SVSG2** ✓	Y.Y.	23:09

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
13	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps: a) CA takes the TEB and plastic case prepared for the CO. b) CO takes their cards from the card holder and places them inside the plastic case. c) CO gives the plastic case containing the cards to the CA. d) CA places the plastic case into its designated new TEB, reads aloud the TEB number and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony inventory. f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. g) CA gives the TEB containing the cards to the CO. h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. i) CO writes the date and time, then signs the table of the IW's script, then the IW initials the entry. j) CO returns to their seat with their TEBs, being especially careful not to compromise any TEB. k) Repeat steps for all the remaining COs' credentials on the list. **CO1: Arbogast Fabian** **Set # 1 TEB # BB02638503** ✓ **CO2: Ralf Weber** **Set # 1 TEB # BB02638504** ✓ **CO3: João Damas** **Set # 1 TEB # BB02638512** ✓ **CO6: Jorge Etges** **Set # 1 TEB # BB02638505** ✓ **CO7: Subramanian Moonesamy** **Set # 1 TEB # BB02638506** ✓	Y.Y.	23:18

CO	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	Set # 1 TEB # **BB02638503**	**Arbogast Fabian**		**2023 Jul** 19	23:13	Y.Y.
CO2	Set # 1 TEB # **BB02638504**	**Ralf Weber**		**2023 Jul** 19	23:14	Y.Y.
CO3	Set # 1 TEB # **BB02638512**	**João Damas**		**2023 Jul** 19	23:15	Y.Y.
CO6	Set # 1 TEB # **BB02638505**	**Jorge Etges**		**2023 Jul** 19	2316	Y.Y.
CO7	Set # 1 TEB # **BB02638506**	**Subramanian Moonesamy**		**2023 Jul** 19	2317	Y.Y.

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

Step	Activity	Initials	Time
14	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)	Y.Y.	23:19
15	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.**	Y.Y.	23:20
16	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.**	Y.Y.	23:21
17	CA performs the following steps to return each piece of equipment to the safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where **"Return"** is indicated. d) IW verifies the safe log entry, then initials it. **HSM5W: TEB # BB51184282** ✓ **HSM6W: TEB # BB51184283** ✓ **HSM7W: TEB # BB51184280** ✓ **Laptop4: TEB # BB81420076** ✓ **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638508** ✓ **KSK-2023: TEB # BB02638507**✓	Y.Y.	23:24

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
18	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.	Y.Y.	23:25
19	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	Y.Y.	23:25
20	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	Y.Y.	23:26

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
21	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)	Y.Y.	23:26
22	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.**	Y.Y.	23:27
23	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.**	Y.Y.	23:28

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

Step	Activity	Initials	Time
24	COs perform the following steps sequentially to return the listed TEBs: a) CO reads aloud the TEB number(s), then verifies integrity while showing the TEB(s) to the audit camera above b) After the CA operates the guard key in the bottom lock, CO reads aloud the safe deposit box number and uses their tenant key to operate the top lock. c) CO opens their safe deposit box, places their TEB(s) inside, then closes and locks the safe deposit box. d) CO writes the date and time, then signs the safe log where **"Return"** is indicated. e) IW verifies the completed safe log entry, then initials it. **CO1: Arbogast Fabian** **Box # 1788** **Set # 1 TEB # BB02638503** ✓ **CO2: Ralf Weber** **Box # 1071** **Set # 1 TEB # BB02638504** ✓ **CO3: João Damas** **Box # 1069** **Set # 1 TEB # BB02638512** ✓ **CO6: Jorge Etges** **Box # 1072** **Set # 1 TEB # BB02638505** ✓ **CO7: Subramanian Moonesamy** **Box # 1790** **Set # 1 TEB # BB02638506** ✓	Y.Y.	23:35

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
25	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.	Y.Y.	23:35
26	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.	Y.Y.	23:36
27	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	Y.Y.	23:36

Act 8: 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.	Y.Y.	23:37
2	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.**	Y.Y.	23:42
3	CA reviews IW's script, then signs the participants list.	Y.Y.	23:44
4	IW signs the list and records the completion time.	Y.Y.	23:44

Stop Online Streaming and Recording

Step	Activity	Initials	Time
5	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.	Y.Y.	23:45
6	CA requests that an SA stop the audit camera video recording.	Y.Y.	23:46
7	CA informs onsite participants of post ceremony activities.	Y.Y.	23:46
8	Ceremony participants take a group photo.	Y.Y.	23:49

Sign Out of Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
9	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.)	Y.Y.	23:59

Bundle Audit Materials

Step	Activity	Initials	Time
10	IW makes a copy of their script for off-site audit bundle containing: a) Output of signer system - HSMFD. b) Copy of IW's key ceremony script. c) Audio-visual recording from the audit cameras. d) Logs from the Physical Access Control System and Intrusion Detection System: Range: **20220201 00:00:00 to 20230720 00:00:00 UTC** e) IW's attestation (See Appendix C on page 42). f) SA's attestation (See Appendix D on page 43 and Appendix E on page 44). All TEBs are labeled **Root DNSSEC KSK Ceremony 50**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	Y.Y.	+1 00:45

Appendix A: Glossary

[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] **configure-printer:*** A bash script used to install the HP LaserJet print driver from the command line instead of **system-config-printer**.

[3] **copy-hsmfd:*** A bash script used to copy HSMFD contents to new flash drives; includes verification via hash comparison.

[4] **hsmfd-hash:*** A bash script used to calculate, print, and compare SHA-256 checksums for the HSMFD flash drives.

Note: The sort command has different behavior depending on the locale settings specified by environment variables. Current OS locale setting is `LC_COLLATE="POSIX"`

[5] **kskm-keymaster:**** An application that creates and deletes keys and performs a key inventory.

[6] **kskm-ksrsigner:**** An application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.

[7] **ksrsigner:** A legacy application that 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-legacy

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

[9] **printlog:*** A bash script used to print the Key Signing Log output from **ksrsigner** application.

[10] **print-script:*** A bash script used to print the terminal commands.

[11] **print-ttyaudit:*** A bash script used to print the HSM logs.

[12] **sha2wordlist:** An application that reads data from STDIN and outputs a SHA-256 checksum as hex and PGP words in STDOUT.

The source code is available at https://github.com/kirei/sha2wordlist

[13] **ttyaudit:*** A perl script used to capture and log the HSM output.

---

* The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-1.0.0coen_amd64.deb
A debian package is an **ar** archive. To extract data from a deb package, use the command **ar -x ksk-tools-1.0.0coen_amd64.deb**
Then extract the files with **tar -xvf data.tar.xz**
The file will be located in the directory: **./opt/icann/bin/**

** The source code is available at https://github.com/iana-org/dnssec-keytools

[14] **Keyper HSM Role Cards:**

a) **OP (Operator):** Configures the HSM to an online or offline state toggling communication through its ethernet adapter. Required for communication with the laptop for key signing operations.

b) **SO (Security Officer):** Used for HSM administrative operations. Required to create other role cards (OP and CO), and the introduction or zeroization of an HSM.

c) **CO (Crypto Officer):** Used for the key management functions in an HSM. Required for adding or deleting keys stored in an HSM.

d) **SMK (Storage Master Key):** Allows an HSM to read an encrypted APP key backup. Required for initial migration of keys and disaster recovery.

e) **AAK (Adapter Authorization Key):** Configures an HSM to use previously generated OP, CO, and SO cards. Required for the introduction of an HSM.

f) **APP (Application Key):** An encrypted backup copy of one or more keys stored in an HSM, which can only be decoded by its corresponding SMK. Required for migrating keys and disaster recovery.

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 generated during the ceremony, and attestation. See Appendix C on page 42.

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 43.

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

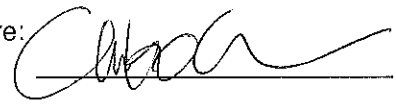
7. Other items

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 Yokoyama**

Signature: 

Date: 2023 Jul 19

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:

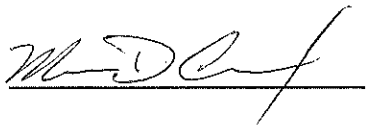
a) There were NO discrepancies found in the system configurations, assigned authorizations, and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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: **20220201 00:00:00 to 20230720 00:00:00 UTC.**

SA: Moises D. Cinilo

Signature: 

Date: 2023 Jul 19

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: Moises D. Cirilo

Signature:

Date: 2023 Jul 19

```
## Last commit: 2021-12-14 19:29:53 UTC by root
version 19.4R3-S1.3;
system {
    host-name srx;
    root-authentication {
        encrypted-password "XXXX"; ## SECRET-DATA
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user mcirilo {
            full-name "Moises D. Cirilo";
            uid 2006;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2008;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user sfreeark {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        password {
            format sha512;
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    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;
        }
    }
    name-server {
        192.0.42.53;
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
chassis {
    config-button no-rescue no-clear;
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
security {
    pki {
        ca-profile root-ca {
            ca-identity "ICANN Root CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
            administrator {
                email-address "cbo-team@iana.org";
            }
        }
        ca-profile intermediate-ca {
            ca-identity "ICANN SSL CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
        }
    }
    ike {
        proposal ike-proposal-KMF {
            authentication-method rsa-signatures;
```

```
        dh-group group24;
        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
    }
    policy ike-policy-KMF {
        proposals ike-proposal-KMF;
        certificate {
            local-certificate ksk-iax;
        }
    }
    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 EVH IMS ];
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVH 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 192.8.42.53/32;
        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;
    }
}
}
policy-options {
prefix-list resolver-servers {
    apply-path "system name-server <*>";
}
prefix-list local-prefixes {
    10.4.28.0/24;
}
prefix-list ntp-servers {
    129.6.15.28/32;
    129.6.15.29/32;
}
prefix-list remote-ike-peers {
    apply-path "security ike gateway <*> address <*>";
}
}
firewall {
family inet {
    filter route-engine-filter {
        term deny-icmp-redirects {
            from {
                protocol icmp;
                icmp-type redirect;
            }
            then {
                discard;
            }
        }
        term allow-icmp {
            from {
                protocol icmp;
                icmp-type [ echo-request echo-reply unreachable time-exceeded ];
            }
            then {
                policer small-bw-limit;
                accept;
            }
        }
        term allow-traceroute {
            from {
                protocol udp;
                port 33434-33534;
            }
            then {
                policer small-bw-limit;
                accept;
            }
        }
        term allow-dns {
            from {
                source-prefix-list {
                    resolver-servers;
                }
                protocol udp;
                source-port domain;
            }
            then {
                policer small-bw-limit;
                accept;
            }
        }
        term allow-ntp {
            from {
                source-prefix-list {
                    local-prefixes;
                    ntp-servers;
                }
                protocol udp;
                port ntp;
            }
            then {
                policer small-bw-limit;
                accept;
            }
        }
        term allow-establish {
            from {
                protocol tcp;
                tcp-established;
```

```
            }
            then accept;
        }
        term allow-ipsec-esp {
            from {
                source-prefix-list {
                    remote-ike-peers;
                }
                protocol esp;
            }
            then accept;
        }
        term allow-ipsec-udp {
            from {
                source-prefix-list {
                    remote-ike-peers;
                }
                protocol udp;
                port 500;
            }
            then accept;
        }
        term allow-ike-fragments {
            from {
                source-prefix-list {
                    remote-ike-peers;
                }
                is-fragment;
                protocol udp;
            }
            then {
                policer small-bw-limit;
                accept;
            }
        }
        term allow-ssh {
            from {
                source-address {
                    10.4.29.193/32;
                }
                protocol tcp;
                destination-port ssh;
            }
            then accept;
        }
        term LAST {
            then {
                discard;
            }
        }
    }
}
policer small-bw-limit {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 15k;
    }
    then discard;
}
}
vlans {
    vlan-access {
        vlan-id 10;
        l3-interface irb.0;
    }
    vlan-guest {
        vlan-id 12;
        l3-interface irb.2;
    }
    vlan-video {
        vlan-id 11;
        l3-interface irb.1;
    }
    vlan-wifi {
        vlan-id 13;
        l3-interface irb.3;
    }
}
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;
    }
}
```