Root DNSSEC KSK Ceremony 51

Thursday 30 November 2023

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

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

Abbreviations

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

Participants

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

Title / Roles	Printed Name	Signature	Date	Time
CA	David Huberman / ICANN		2023 Nov 30	22:32
IW	Andy Newton / ICANN			
SSC1	Rob Hoggarth / ICANN			
SSC2	Hope Shafer / ICANN			
CO1	Frederico Neves			
CO2	Pia Gruvö			
CO4	Robert Seastrom			
CO5	Nomsa Mwayenga			
CO6	Hugo Salgado			
RZM	Trevor Davis / Verisign			
AUD	Melanie Chen / RSM			
AUD	Grant Noah An / RSM			
SA	Darren Kara / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Butch Pfremmer / ICANN			
SW	Ariel Liang / ICANN			
SW	James Mitchell / PTI			
EW	Nick Kotakis			
EW	Lodrina Cherne			

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.		18:00
2	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2.		18:01
3	CA asks that any first time ceremony participants in the room introduce themselves.		18:03

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.		18:03
5	CA explains the use of personal electronic devices during the ceremony.		18:04
6	CA summarizes the purpose of the ceremony.		18:06

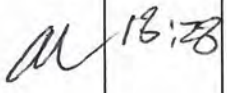
Verify the Time and Date

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: 2023-11-30 18:06 **Note: All entries into this script or any logs should follow this common source of time.**		18:06

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.)		18:10
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.**		18:12
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.		18:13

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. **Note 1: The CO's key will remain inserted in their assigned safe deposit box lock when specified below.** **Note 2: The COs will retrieve their new safe deposit box keys when specified below.** e) CO writes the date and time, then signs the safe log. f) IW verifies the completed safe log entries, then initials them. **CO1: Frederico Neves** **Box # 1239** **Set # 1 TEB # BB02639501** (Retain) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02638534** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO2: Pia Gruvö** **Box # 1264** **Set # 1 TEB # BB02639500** (Retain) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02639498** (Check and Return) Last Verified: KSK Ceremony 45 2022-05-12 **CO4: Robert Seastrom** **Box # 1260** (Key shall remain in lock) **New Box # 1243** (Retrieve keys from lock) **OP TEB # BB91951237** (Retain) **SO TEB # BB02639553** (Retain) **Set # 1 TEB # BB02639552** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02639551** (Transfer to newly assigned safe deposit box) Last Verified: KSK Ceremony 45 2022-05-12 **CO5: Nomsa Mwayenga** **Box # 1262** **Set # 1 TEB # BB02639496** (Retain) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02639548** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO6: Hugo Salgado** **Box # 1242** **Set # 1 TEB # BB02638531** (Retain) Last Verified: KSK Ceremony 49 2023-04-27 **Set # 2 TEB # BB02638530** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **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.**		18:28

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.		18:28
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.		18:29
14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).		18:30

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.)		18:30
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.**		18:32
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.		18:33

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. **HSM5E: TEB # BB51184606 (Place on Cart)** Last Verified: KSK Ceremony 49 2023-04-27 **HSM6E: TEB # BB51184243 (Check and Return)** Last Verified: KSK Ceremony 49 2023-04-27 **HSM7E: TEB # BB51184253 (Place on Cart)** Last Verified: AT Ceremony 51 2023-11-29 **HSM8E: TEB # BB51184254 (Place on Cart)** Last Verified: AT Ceremony 51 2023-11-29 **Laptop3: TEB # BB97448418 (Check and Return)** Last Verified: KSK Ceremony 49 2023-04-27 **Laptop4: TEB # BB81420064 (Place on Cart)** Last Verified: KSK Ceremony 47 2022-11-03 **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638528 (Place on Cart)** Last Verified: KSK Ceremony 49 2023-04-27 **KSK-2017: TEB # BB46584614 (Place on Cart)** Last Verified: KSK Ceremony 43 2021-10-14 **KSK-2023: TEB # BB02638526 (Place on Cart)** Last Verified: KSK Ceremony 49 2023-04-27 **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.**	MH	18:40

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.	MH	18:40
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.	MH	18:41
21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	MH	18:41

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 2 Step(s): 1 Page(s): 10 Date and Time: 30 Nov 2023 19:42 **Note: IW describes the exception(s) and action(s) below.**	AM	18:42

Melanie Chen was escorted out of tier 3 by Andres Pavez.

Act 2: 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. **HSM5E: TEB # BB51184606 / Serial # H1903018** Last Verified: KSK Ceremony 49 2023-04-27 **Laptop4: TEB # BB81420064 / Service Tag # 58SVSG2** Last Verified: KSK Ceremony 47 2022-11-03 **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638528** Last Verified: KSK Ceremony 49 2023-04-27 **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.**		
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.		
3	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 # 2**		
4	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 # 2**. f) Switch it ON.		
5	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**		

OS Media Checksum Verification

Step	Activity	Initials	Time

6	CA uses the terminal window to executes the following steps:
	a) Verify the byte count of the SD card matches the ISO size of 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/51
		AL	18:55

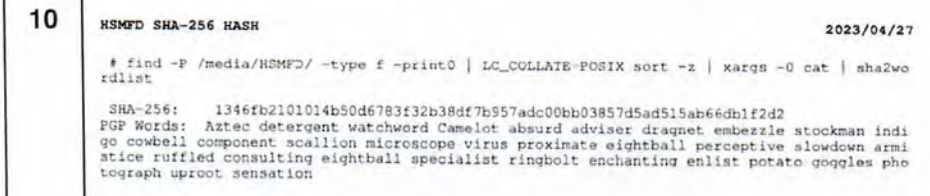
Printer Setup

Step	Activity	Initials	Time
7	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`	AL	18:55

Date Setup

Step	Activity	Initials	Time
8	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 "20231130 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.	AL	18:56

Connect the HSMFD

Step	Activity	Initials	Time
9	CA plugs the **Ceremony 49 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.		18:57
10	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 2023/04/27 # 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 using the printed HSMFD hash from the Ceremony 49 OS Media bundle.		18:59

Distribute Previous HSMFD

Step	Activity	Initials	Time
11	CA gives the unused **HSMFD 49** and the sheet of paper with the printed HSMFD hash to RKOS.		19:00

Start the Terminal Session Logging

Step	Activity	Initials	Time
12	CA executes the command below using the terminal window to change the working directory to HSMFD: `cd /media/HSMFD`		19:00
13	CA executes the command below to log activities of the **Commands** terminal window: `script script-20231130.log`		19:00

Start the HSM Output Logging

Step	Activity	Initials	Time

14	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.
			19:01

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
15	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM5E**. 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 **H1903018**. e) Scroll down to the end of the logging screen. **HSM5E: Serial # H1903018** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	AR	19:03

Act 3: 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 generated 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: Frederico Neves** **Set # 1 TEB # BB02639501** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 47 2022-11-03 **CO2: Pia Gruvö** **Set # 1 TEB # BB02639500** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 47 2022-11-03 **CO4: Robert Seastrom** **OP TEB # BB91951237** (Place the plastic case on the table for destruction) **SO TEB # BB02639553** (Place the plastic case on the table for destruction) **Set # 1 TEB # BB02639552** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 **CO5: Nomsa Mwayenga** **Set # 1 TEB # BB02639496** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02639548** (Place the plastic case on the table for TEB change) Last Verified: KSK Ceremony 45 2022-05-12 **CO6: Hugo Salgado** **Set # 1 TEB # BB02638531** (Place the cards on the designated card holder) Last Verified: KSK Ceremony 49 2023-04-27 **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.**		19:15

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.		
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 6 of 7 2nd OP card 5 of 7 3rd OP card 4 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].**	AW	19:18

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
3	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	AW	19:18

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`
		AW	19:19

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.**	AW	19:20

Execute the KSR Signer for KSR 2024 Q1

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to change directory: `cd /media/KSRFD/KSK51/`	AW	19:20
7	CA executes the command below in the terminal window to sign the KSR file: `kskm-ksrsigner`	AW	19:20

January 18, 2023

VERISIGN

To Whom It May Concern:

This is a letter of Verification of Employment for Trevor Davis. VeriSign, Inc. ("Verisign") has employed Trevor Davis full-time/40 hours per week since September 29, 2014, currently as a Manager - Engineering in Verisign's Production Operations 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 25 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 163.7 million .com and .net domain names and processing more than 219 billion query transactions daily-keeping the world connected online, seamlessly and securely. Verisign is experienced in and provides support for both IPv6 and DNSSEC.

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

Sincerely,

X Dave Carney January 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

30 November 2023

The SHA256 hash of the 2024 Q1 KSR file is:

ksr-root-2024-q1-0.xml:

d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5

The PGP wordlist for the hash above is:

PGP Words: stapler businessman prefer unicorn breadline specialist breakup gossamer cranky pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist amusement crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visitor

Attested on behalf of VeriSign by:

Trevor Davis
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

```
Loaded configuration from file ksrsigner.yaml SHA-256 0f716d1970db983479735e132e858eeea2dae3e250f0cec
ca41335e94cd43350 WORDS artist hideaway goggles bottomless guidance suspicious printer confidence jaw
bone hurricane eyeglass barbecue buzzard leprosy orca universe rebirth surrender tissue tomorrow drum
beat upcoming spyglass revolver regain barbecue chopper ultimate drainage souvenir chisel embezzle
Configuration validated
Loaded SKR from file skr-root-2023-q4-0.xml SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9
ff119e6cc5aed49 WORDS klaxon intention Neptune Virginia skullcap pharmacy ammo hesitate uproot getawa
y retouch inventive trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getawa
y unearth existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
Previous SKR:
#  Inception           Expiration          ZSK Tags      KSK(CKA_LABEL)
1  2023-10-01T00:00:00 2023-10-22T00:00:00  11019,46780   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
Loaded KSR from file ksr-root-2024-q1-0.xml SHA-256 d31f96ec28d5296641aad3bced5fec3675f9e7675a074032b
e83ab9070232af5 WORDS stapler businessman prefer unicorn breadline specialist breakup gossamer cranky
 pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist am
usement crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visitor
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  2024-01-01T00:00:00 2024-01-22T00:00:00  30903,46780
2  2024-01-11T00:00:00 2024-02-01T00:00:00  30903
3  2024-01-21T00:00:00 2024-02-11T00:00:00  30903
4  2024-01-31T00:00:00 2024-02-21T00:00:00  30903
5  2024-02-10T00:00:00 2024-03-02T00:00:00  30903
```

```
6  2024-02-20T00:00:00 2024-03-12T00:00:00  30903
7  2024-03-01T00:00:00 2024-03-22T00:00:00  30903
8  2024-03-11T00:00:00 2024-04-01T00:00:00  30903
9  2024-03-21T00:00:00 2024-04-11T00:00:00  5613,30903
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:           H1903018
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  2024-01-01T00:00:00 2024-01-22T00:00:00 30903,46780   20326(Klajeyz)/S
2  2024-01-11T00:00:00 2024-02-01T00:00:00 30903         20326(Klajeyz)/S
3  2024-01-21T00:00:00 2024-02-11T00:00:00 30903         20326(Klajeyz)/S
4  2024-01-31T00:00:00 2024-02-21T00:00:00 30903         20326(Klajeyz)/S
5  2024-02-10T00:00:00 2024-03-02T00:00:00 30903         20326(Klajeyz)/S
6  2024-02-20T00:00:00 2024-03-12T00:00:00 30903         20326(Klajeyz)/S
7  2024-03-01T00:00:00 2024-03-22T00:00:00 30903         20326(Klajeyz)/S
8  2024-03-11T00:00:00 2024-04-01T00:00:00 30903         20326(Klajeyz)/S
9  2024-03-21T00:00:00 2024-04-11T00:00:00 30903,5613    20326(Klajeyz)/S
Wrote SKR to file skr-root-2024-q1-0.xml SHA-256 0f2922c76d8ac758dedff603d0c2e44e13369c1938d56ef75094
25abf8f0b48f WORDS artist certify blockade retraction goggles maverick soybean everyday tactics thera
pist village aggregate stagnate repellent tonic distortion Aztec congregate python bottomless classic
  specialist goldfish voyager drumbeat molecule bombast Pegasus Vulcan upcoming scenic midsummer
```

Verify the KSR Hash for KSR 2024 Q1

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.** Trevor Davis 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.		
9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		19:23
10	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The SKR is located in: `/media/KSRFD/KSK51/skr-root-2024-q1-0.xml`		19:24

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 kskm-ksrsigner-202311*.log X` **Note: Replace "X" with the amount of copies needed for the participants.**		19:26
12	IW attaches a copy of the required ksr signer log to their script.		19:26

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
13	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 2 of 7 2nd OP card 1 of 7 3rd OP 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].**	AW	19:29

OS Media Checksum Verification

Step	Activity	Initials	Time

14	CA uses the terminal window to executes the following steps:
	a) Verify the byte count of the SD card matches the ISO size of 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/51
		AM	19:31

Act 4: 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 **"3"**, 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) 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 5 of 7 2nd SO card 1 of 7 3rd SO 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].**	M	19:39
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.	M	19:41

Act 5: Issue Temporary Adapter Authorization Key (AAK) Cards

When a ceremony includes the introduction of a new HSM, it is necessary to generate temporary AAK cards to allow existing CO credentials perform signing and administrative operations in the new HSM. These temporary cards will be used and subsequently destroyed before the completion of the ceremony.

Note: For a summary of card roles and their purpose see Appendix A number [14].

Issue Temporary Adapter Authorization Key (AAK) Cards

Step	Activity	Initials	Time
1	CA performs the following steps to issue temporary Adapter Authorization Key (AAK) 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 **"3.Backup AAK"**, press **ENT** to confirm. i) When **"Backup AAK?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. k) When **"Insert Card #X?"** is displayed, insert the required AAK card. l) When **"Remove Card?"** is displayed, remove the AAK card. m) Repeat steps k) to l) for the 2nd AAK card. n) When **"Done AAK"** is displayed, press **ENT** to confirm. o) Press **CLR** to return to the 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 2 of 7 2nd SO card 4 of 7 3rd SO 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].**	AW	19:45

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
2	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.**		19:47
3	CA places the HSM into its designated new TEB, then seals it.		19:48
4	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. **HSM5E: TEB # BB51184250 / Serial # H1903018**		19:49

Act 6: Introduce New HSM

The CA will introduce a new HSM by performing the following steps:

- Verify new HSM serial number
- Import the Adapter Authorization Key (AAK)
- Configure the HSM to a secure state
- Change and verify API settings
- Import Storage Master Key (SMK)
- Import App Key (KSK)
- Verify connectivity, activate, and initialize HSM
- Destroy temporary AAK cards

HSM7E (Tier 7) Setup

Step	Activity	Initials	Time
1	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. **HSM7E: TEB # BB51184253 / Serial # H2110009** Last Verified: AT Ceremony 51 2023-11-29 **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.**		19:51

Power ON the HSM7E (Tier 7)

Step	Activity	Initials	Time
2	CA selects the **HSM Output** terminal window.		19:51
3	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM7E**. 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 **H2110009**. e) Scroll down to the end of the logging screen. f) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**		19:53

Import the AAK

Step	Activity	Initials	Time
4	CA performs the following steps to import the Adapter Authorization Key (AAK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Restore AAK"**, press **ENT** to confirm. c) When **"Restore AAK?"** is displayed, press **ENT** to confirm. d) When **"Insert Card #X?"** is displayed, insert the required AAK card and press **ENT**. e) When **"Remove Card?"** is displayed, remove the AAK card. f) Repeat steps d) to e) for the 2nd AAK card. g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm. Each card is returned to its designated card holder after use. **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].**	MR	19:54

Configure the HSM to Secure State

Step	Activity	Initials	Time
5	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.Secure"**, press **ENT** to confirm. c) When **"Secure?"** is displayed, 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 cards. h) When **"SMK AES Triple DES?"** is displayed, press **CLR** to skip. i) When **"SMK AES"** is displayed, press **ENT** to confirm. j) When **"LAN Port Number?"** is displayed, press **CLR** to skip. k) When **"Enable IPv4/IPv6?"** is displayed, press **CLR** to skip. l) When **"LAN IPv4 Address?"** is displayed, press **CLR** to skip. m) When **"LAN IPv4 Mask?"** is displayed, press **CLR** to skip. n) When **"Set IPv4 Gateway?"** is displayed, press **CLR** to skip. o) When **"LAN IPv6 Address?"** is displayed, press **CLR** to skip. p) When **"LAN IPv6 Mask?"** is displayed, press **CLR** to skip. q) When **"Set IPv6 Gateway?"** is displayed, press **CLR** to skip. r) When **"Remote Mgmt Off Enable?"** is displayed, press **CLR** to skip. s) When **"Remote Mgmt Off** is displayed, press **ENT** to confirm. t) When **"Change Clock?"** is displayed, press **CLR** to skip. u) When **"Import Config?"** is displayed, press **CLR** to skip. v) When **"FIPS Mode On Disable?"** is displayed, press **CLR** to skip. w) When **"FIPS Mode On"** is displayed, press **ENT** to confirm. x) When **"Global Key Export Enabled"** is displayed, press **CLR** to skip. **Done Rebooting Device** will be displayed. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st SO card 4 of 7 2nd SO card 5 of 7 3rd SO card 2 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].**		

Change the API Settings

Step	Activity	Initials	Time
6	CA performs the following steps to change the API settings: 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. g) Select **"5. API Settings"**, press **ENT** to confirm. h) Select **"1.Key Import"**, press **ENT** to confirm. i) When **"Key Import On Disable?"** is displayed, press **ENT** to confirm. j) Select **"2.Key Export"**, press **ENT** to confirm. k) When **"Key Export On Disable?"** is displayed, press **ENT** to confirm. l) Select **"5.Sym Key Der"**, press **ENT** to confirm. m) When **"Sym Key Der On Disable?"** is displayed, press **ENT** to confirm. n) Press **CLR twice** 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 CO card 1 of 7 2nd CO card 4 of 7 3rd CO card 5 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].**	dm	20:00

Verify API Settings

Step	Activity	Initials	Time

7	CA performs the following steps to dump the status of the HSM:
	a) Utilize the HSM's keyboard to scroll through the menu using < >
	b) Select **"4.HSM Info"**, press **ENT** to confirm.
	c) Select **"8.Output Info"**, press **ENT** to confirm.
	d) When **"Output Info?"** is displayed, press **ENT** to confirm.
	e) Press **CLR** to return to the main menu **"Secured"**.
	
	CA selects the **HSM Output** terminal window and scrolls up to confirm with IW the output of the HSM configuration matches with the list below:
	
	`Modes: (1=Enabled 0=Disabled)`
	`Global Key Export 1`
	`App Key Import 0`
	`App Key Export 0`
	`Asymmetric Key Gen 1`
	`Symmetric Key Gen 1`
	`Symmetric Key Derive 0`
	`Signing 1`
	`Signature Verify 1`
	`MAC Generation 1`
	`MAC Verification 1`
	`Encrypt / Decrypt 1`
	`Delete Asym Key 1`
	`Delete Sym Key 1`
	`Output Key Details 1`
	`Output Key Summary 1`
	`Suite B Algorithms 1`
	`Non Suite B Algs 1`
	`Auto Online 0`
	`Remote Management 0`
	`AES SMK`
	`Set Offline`
	`FIPS Mode`
		AM	20:02

App Key Backups

Step	Activity	Initials	Time
8	CA performs the following steps to prepare the App key backups: 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 App key cards and the backup HSMFD on its designated area of the ceremony table. e) If not already present, place corresponding labels on the APP key plastic case and ensure their respective HSMFDs remain in the plastic case. **KSK-2017: TEB # BB46584614** Last Verified: KSK Ceremony 43 2021-10-14 **KSK-2023: TEB # BB02638526** Last Verified: KSK Ceremony 49 2023-04-27 **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.**	AM	20:08

Import the SMK and the KSK

Step	Activity	Initials	Time
9	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 6 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].**	AR	20:10

Step	Activity	Initials	Time
10	CA performs the following steps to import the SMK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"3.Restore SMK"**, press **ENT** to confirm. d) When **"Restore SMK?"** is displayed, press **ENT** to confirm. e) When **"Insert Card SMK #X?"** is displayed, insert the SMK card. f) When **"Remove Card?"** is displayed, remove the SMK card. g) Repeat steps e) to f) for the 2nd and 3rd SMK card. h) When **"SMK Restored"** is displayed, press **ENT** to confirm. i) Press **CLR** once to return to the menu **"Key Mgmt"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st SMK card 6 of 7 2nd SMK card 4 of 7 3rd SMK card 5 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].**		20:12
11	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) Repeat steps c) to h) for any remaining App Key card listed below. j) Press **CLR twice** to return to the main menu **"Secured"**. CA uses the card listed below. Card is returned to its designated card holder after use. **KSK-2017: Klajeyz** App Key card # **1** **KSK-2023: Kmrfl3b** App Key card # **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].**		20:14

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
12	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st OP card 1 of 7 2nd OP card 5 of 7 3rd OP card 2 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].**	AM	20:16

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
13	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	AM	20:16

14	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`
		AM	20:16

Execute the KSR Signer for KSR 2024 Q1

Step	Activity	Initials	Time
15	CA executes the command below in the terminal window to change directory: `cd HSM7E/`	AM	20:17
16	CA executes the command below in the terminal window to sign the KSR file: `kskm-ksrsigner`	AM	20:17

```
Loaded configuration from file ksrsigner.yaml SHA-256 432a513b007acc8ae97057bccefca01f36dd334d00e7cac
0462df3abc3a69388 WORDS crucial chambermaid drunken councilman aardvark infancy spigot maverick tread
mill hesitate eightball pyramid spyglass Wilmington ragtime businessman Christmas tambourine chisel d
isruptive aardvark truncated spellbind recipe cubic clergyman upset Pegasus snowcap paragon playhouse
 maritime
Configuration validated
Loaded SKR from file skr-root-2023-q4-0.xml SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9
ff119e6cc5aed49 WORDS klaxon intention Neptune Virginia skullcap pharmacy ammo hesitate uproot getawa
y retouch inventive trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getawa
y unearth existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
Previous 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
Loaded KSR from file ksr-root-2024-q1-0.xml SHA-256 d31f96ec28d5296641aad3bced5fec3675f9e7675a074032b
e83ab9070232af5 WORDS stapler businessman prefer unicorn breadline specialist breakup gossamer cranky
 pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist am
usement crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visitor
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  2024-01-01T00:00:00 2024-01-22T00:00:00  46780,30903
2  2024-01-11T00:00:00 2024-02-01T00:00:00  30903
3  2024-01-21T00:00:00 2024-02-11T00:00:00  30903
4  2024-01-31T00:00:00 2024-02-21T00:00:00  30903
```

```
5  2024-02-10T00:00:00 2024-03-02T00:00:00  30903
6  2024-02-20T00:00:00 2024-03-12T00:00:00  30903
7  2024-03-01T00:00:00 2024-03-22T00:00:00  30903
8  2024-03-11T00:00:00 2024-04-01T00:00:00  30903
9  2024-03-21T00:00:00 2024-04-11T00:00:00  5613,30903
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:           H2110009
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  2024-01-01T00:00:00 2024-01-22T00:00:00  46780,30903   20326(Klajeyz)/S
2  2024-01-11T00:00:00 2024-02-01T00:00:00  30903         20326(Klajeyz)/S
3  2024-01-21T00:00:00 2024-02-11T00:00:00  30903         20326(Klajeyz)/S
4  2024-01-31T00:00:00 2024-02-21T00:00:00  30903         20326(Klajeyz)/S
5  2024-02-10T00:00:00 2024-03-02T00:00:00  30903         20326(Klajeyz)/S
6  2024-02-20T00:00:00 2024-03-12T00:00:00  30903         20326(Klajeyz)/S
7  2024-03-01T00:00:00 2024-03-22T00:00:00  30903         20326(Klajeyz)/S
8  2024-03-11T00:00:00 2024-04-01T00:00:00  30903         20326(Klajeyz)/S
9  2024-03-21T00:00:00 2024-04-11T00:00:00  5613,30903    20326(Klajeyz)/S
Wrote SKR to file HSM7E-skr-root-2024-q1-0.xml SHA-256 0f2922c76d8ac758dedff603d0c2e44e13369c1938d56e
f7509425abf8f0b48f WORDS artist certify blockade retraction goggles maverick soybean everyday tactics
 therapist village aggregate stagnate repellent tonic distortion Aztec congregate python bottomless c
lassic specialist goldfish voyager drumbeat molecule bombast Pegasus Vulcan upcoming scenic midsummer
```

Verify the KSR Hash for KSR 2024 Q1

Step	Activity	Initials	Time
17	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.		20:19
18	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		20:19
19	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The SKR is located in: `/media/KSRFD/KSK51/HSM7E/HSM7E-skr-root-2024-q1-0.xml`		20:19

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
20	CA executes the commands below using the terminal window to print the KSR Signer log: a) `printlog kskm-ksrsigner-202311*.log X` **Note: Replace "X" with the amount of copies needed for the participants.**		20:21
21	IW attaches a copy of the required ksr signer log to their script.		20:21

SKR Comparison

Step	Activity	Initials	Time
22	CA executes the command below to display the `XSL` style sheet content: `cat style.xsl`		20:22
23	CA executes the commands below using the terminal window to compare the SKRs: a) `xsltproc style.xsl ../skr-root-2024-q1-0.xml | xmllint --format - > current` b) `xsltproc style.xsl HSM7E-skr-root-2024-q1-0.xml | xmllint --format - > new` c) `diff -wu current new`		20:23
24	CA executes the command below in the terminal window to change directory: `cd ..`		20:23

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
25	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 5 of 7 2nd OP card 6 of 7 3rd OP card 2 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].**	AM	20:25

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
26	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.**	AM	20:26
27	CA places the HSM into its designated new TEB, then seals it.	AM	20:27
28	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. **HSM7E: TEB # BB51184251 / Serial # H2110009**	AM	20:28

HSM8E (Tier 7) Setup

Step	Activity	Initials	Time
29	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. **HSM8E: TEB # BB51184254 / Serial # H2110010** Last Verified: AT Ceremony 51 2023-11-29 **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.**	M	20:30

Power ON the HSM8E (Tier 7)

Step	Activity	Initials	Time
30	CA selects the **HSM Output** terminal window.	M	20:30
31	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM8E**. 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 **H2110010**. e) Scroll down to the end of the logging screen. f) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	M	20:31

Import the AAK

Step	Activity	Initials	Time
32	CA performs the following steps to import the Adapter Authorization Key (AAK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Restore AAK"**, press **ENT** to confirm. c) When **"Restore AAK?"** is displayed, press **ENT** to confirm. d) When **"Insert Card #X?"** is displayed, insert the required AAK card and press **ENT**. e) When **"Remove Card?"** is displayed, remove the AAK card. f) Repeat steps d) to e) for the 2nd AAK card. 2 of 2 1 of 2 g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm. Each card is returned to its designated card holder after use. **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].**	M	20:32

Configure the HSM to Secure State

Step	Activity	Initials	Time
33	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.Secure"**, press **ENT** to confirm. c) When **"Secure?"** is displayed, 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 cards. h) When **"SMK AES Triple DES?"** is displayed, press **CLR** to skip. i) When **"SMK AES"** is displayed, press **ENT** to confirm. j) When **"LAN Port Number?"** is displayed, press **CLR** to skip. k) When **"Enable IPv4/IPv6?"** is displayed, press **CLR** to skip. l) When **"LAN IPv4 Address?"** is displayed, press **CLR** to skip. m) When **"LAN IPv4 Mask?"** is displayed, press **CLR** to skip. n) When **"Set IPv4 Gateway?"** is displayed, press **CLR** to skip. o) When **"LAN IPv6 Address?"** is displayed, press **CLR** to skip. p) When **"LAN IPv6 Mask?"** is displayed, press **CLR** to skip. q) When **"Set IPv6 Gateway?"** is displayed, press **CLR** to skip. r) When **"Remote Mgmt Off Enable?"** is displayed, press **CLR** to skip. s) When **"Remote Mgmt Off** is displayed, press **ENT** to confirm. t) When **"Change Clock?"** is displayed, press **CLR** to skip. u) When **"Import Config?"** is displayed, press **CLR** to skip. v) When **"FIPS Mode On Disable?"** is displayed, press **CLR** to skip. w) When **"FIPS Mode On"** is displayed, press **ENT** to confirm. x) When **"Global Key Export Enabled"** is displayed, press **CLR** to skip. **Done Rebooting Device** will be displayed. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st SO card 5 of 7 2nd SO card 1 of 7 3rd SO 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].**	M	20:35

Change the API Settings

Step	Activity	Initials	Time
34	CA performs the following steps to change the API settings: 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. g) Select **"5. API Settings"**, press **ENT** to confirm. h) Select **"1.Key Import"**, press **ENT** to confirm. i) When **"Key Import On Disable?"** is displayed, press **ENT** to confirm. j) Select **"2.Key Export"**, press **ENT** to confirm. k) When **"Key Export On Disable?"** is displayed, press **ENT** to confirm. l) Select **"5.Sym Key Der"**, press **ENT** to confirm. m) When **"Sym Key Der On Disable?"** is displayed, press **ENT** to confirm. n) Press **CLR twice** 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 CO card 1 of 7 2nd CO card 4 of 7 3rd CO card 5 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].**	IW	20:37

Verify API Settings

Step	Activity	Initials	Time

35	CA performs the following steps to dump the status of the HSM:
	a) Utilize the HSM's keyboard to scroll through the menu using < >
	b) Select **"4.HSM Info"**, press **ENT** to confirm.
	c) Select **"8.Output Info"**, press **ENT** to confirm.
	d) When **"Output Info?"** is displayed, press **ENT** to confirm.
	e) Press **CLR** to return to the main menu **"Secured"**.
	
	CA selects the **HSM Output** terminal window and scrolls up to confirm with IW the output of the HSM configuration matches with the list below:
	
	`Modes: (1=Enabled 0=Disabled)`
	`Global Key Export 1`
	`App Key Import 0`
	`App Key Export 0`
	`Asymmetric Key Gen 1`
	`Symmetric Key Gen 1`
	`Symmetric Key Derive 0`
	`Signing 1`
	`Signature Verify 1`
	`MAC Generation 1`
	`MAC Verification 1`
	`Encrypt / Decrypt 1`
	`Delete Asym Key 1`
	`Delete Sym Key 1`
	`Output Key Details 1`
	`Output Key Summary 1`
	`Suite B Algorithms 1`
	`Non Suite B Algs 1`
	`Auto Online 0`
	`Remote Management 0`
	`AES SMK`
	`Set Offline`
	`FIPS Mode`
			20:38

Import the SMK and the KSK

Step	Activity	Initials	Time
36	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 5 of 7 2nd CO card 2 of 7 3rd CO card 4 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].**		20:40

Step	Activity	Initials	Time
37	CA performs the following steps to import the SMK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"3.Restore SMK"**, press **ENT** to confirm. d) When **"Restore SMK?"** is displayed, press **ENT** to confirm. e) When **"Insert Card SMK #X?"** is displayed, insert the SMK card. f) When **"Remove Card?"** is displayed, remove the SMK card. g) Repeat steps e) to f) for the 2nd and 3rd SMK card. h) When **"SMK Restored"** is displayed, press **ENT** to confirm. i) Press **CLR** once to return to the menu **"Key Mgmt"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st SMK card 1 of 7 2nd SMK card 2 of 7 3rd SMK 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].**	IW	20:41
38	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) Repeat steps c) to h) for any remaining App Key card listed below. j) Press **CLR twice** to return to the main menu **"Secured"**. CA uses the card listed below. Card is returned to its designated card holder after use. **KSK-2017: Klajeyz** App Key card # **2** **KSK-2023: Kmrfl3b** App Key card # **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].**	IW	20:44

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
39	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st OP card 4 of 7 2nd OP card 1 of 7 3rd OP 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].**	AR	20:46

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
40	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	AR	20:46

41	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`
		AR	20:46

Execute the KSR Signer for KSR 2024 Q1

Step	Activity	Initials	Time
42	CA executes the command below in the terminal window to change directory: `cd HSM8E/`	AR	20:47
43	CA executes the command below in the terminal window to sign the KSR file: `kskm-ksrsigner`	AR	20:47

```
Loaded configuration from file ksrsigner.yaml SHA-256 393blacd14c7dbdb975539ada03d4f7ce4822500c460f6f
3603a7e4ae4fd20b9 WORDS classroom councilman beehive sandalwood baboon retraction suspense suspicious
 preshrunk equipment classroom perceptive ragtime crucifix dropper informant tonic Istanbul bombast a
droitness snowslide fortitude village vertigo facial corrosion locale direction tonic Wyoming bison p
roximate
Configuration validated
Loaded SKR from file skr-root-2023-q4-0.xml SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9
ff119e6cc5aed49 WORDS klaxon intention Neptune Virginia skullcap pharmacy ammo hesitate uproot getawa
y retouch inventive trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getawa
y unearth existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
Previous 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
Loaded KSR from file ksr-root-2024-q1-0.xml SHA-256 d31f96ec28d5296641aad3bced5fec3675f9e7675a074032b
e83ab9070232af5 WORDS stapler businessman prefer unicorn breadline specialist breakup gossamer cranky
 pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist am
usement crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visitor
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  2024-01-01T00:00:00 2024-01-22T00:00:00  46780,30903
2  2024-01-11T00:00:00 2024-02-01T00:00:00  30903
3  2024-01-21T00:00:00 2024-02-11T00:00:00  30903
4  2024-01-31T00:00:00 2024-02-21T00:00:00  30903
```

```
5  2024-02-10T00:00:00 2024-03-02T00:00:00  30903
6  2024-02-20T00:00:00 2024-03-12T00:00:00  30903
7  2024-03-01T00:00:00 2024-03-22T00:00:00  30903
8  2024-03-11T00:00:00 2024-04-01T00:00:00  30903
9  2024-03-21T00:00:00 2024-04-11T00:00:00  30903,5613
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:           H2110010
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  2024-01-01T00:00:00 2024-01-22T00:00:00 46780,30903   20326(Klajeyz)/S
2  2024-01-11T00:00:00 2024-02-01T00:00:00 30903         20326(Klajeyz)/S
3  2024-01-21T00:00:00 2024-02-11T00:00:00 30903         20326(Klajeyz)/S
4  2024-01-31T00:00:00 2024-02-21T00:00:00 30903         20326(Klajeyz)/S
5  2024-02-10T00:00:00 2024-03-02T00:00:00 30903         20326(Klajeyz)/S
6  2024-02-20T00:00:00 2024-03-12T00:00:00 30903         20326(Klajeyz)/S
7  2024-03-01T00:00:00 2024-03-22T00:00:00 30903         20326(Klajeyz)/S
8  2024-03-11T00:00:00 2024-04-01T00:00:00 30903         20326(Klajeyz)/S
9  2024-03-21T00:00:00 2024-04-11T00:00:00 30903,5613    20326(Klajeyz)/S
Wrote SKR to file HSM8E-skr-root-2024-q1-0.xml SHA-256 0f2922c76d8ac758dedff603d0c2e44e13369c1938d56e
f7509425abf8f0b48f WORDS artist certify blockade retraction goggles maverick soybean everyday tactics
 therapist village aggregate stagnate repellent tonic distortion Aztec congregate python bottomless c
lassic specialist goldfish voyager drumbeat molecule bombast Pegasus Vulcan upcoming scenic midsummer
```

Verify the KSR Hash for KSR 2024 Q1

Step	Activity	Initials	Time
44	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.		20:48
45	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**		20:48
46	CA enters **Yes** in response to `"Sign KSR?"` to complete the KSR signing operation. The SKR is located in: `/media/KSRFD/KSK51/HSM8E/HSM8E-skr-root-2024-q1-0.xml`		20:48

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
47	CA executes the commands below using the terminal window to print the KSR Signer log: a) `printlog kskm-ksrsigner-202311*.log X` **Note: Replace "X" with the amount of copies needed for the participants.**		20:50
48	IW attaches a copy of the required ksr signer log to their script.		20:50

SKR Comparison

Step	Activity	Initials	Time
49	CA executes the command below to display the `XSL` style sheet content: `cat style.xsl`		20:51
50	CA executes the commands below using the terminal window to compare the SKRs: a) `xsltproc style.xsl ../skr-root-2024-q1-0.xml | xmllint --format - > current` b) `xsltproc style.xsl HSM8E-skr-root-2024-q1-0.xml | xmllint --format - > new` c) `diff -wu current new`		20:51
51	CA executes the command below in the terminal window to change directory: `cd /media/HSMFD`		20:51

Copy the Newly Generated SKR

Step	Activity	Initials	Time

52	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/KSK51/ /media/KSRFD/KSK51/`
	e) Unmount the KSRFD by executing:
	`umount /media/KSRFD`		

53	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.**		

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
54	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 2 of 7 2nd OP card 5 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].**		

Clear and Destroy AAK Cards

Step	Activity	Initials	Time
55	CA performs the following steps to clear Adapter Authorization Key (AAK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps d) to f) for the 2nd and 3rd SO card. g) Select **"5.Clear AAK Card"**, press **ENT** to confirm. h) When **"Clear AAK Card?"** is displayed, press **ENT** to confirm. i) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. j) When **"Insert Card AAK #X?"** is displayed, take the **AAK #X** card from the cardholder, show the **AAK #X** card to the audit camera and then insert the **AAK #X** card into the HSM's card reader. k) When **"Are you sure?"** is displayed, press **ENT** to confirm. l) When **"Remove Card?"** is displayed, remove the AAK card. m) Repeat steps j) to l) for the 2nd AAK card. n) Press **CLR** to return to the main menu **"Secured"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st SO card 4 of 7 2nd SO card 1 of 7 3rd SO 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].**		20:57
56	CA uses the shredder to destroy the cleared AAK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.		21:00

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
57	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.**		21:01
58	CA places the HSM into its designated new TEB, then seals it.		21:02
59	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. **HSM8E: TEB # BB51184252 / Serial # H2110010**		21:03

Return the KSK into a TEB

Step	Activity	Initials	Time
60	CA places the KSK and the backup HSMFD into its designated new TEB, then seals it.		21:07
61	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the KSK TEB on the cart. **KSK-2017: TEB # BB02638662** **KSK-2023: TEB # BB02638661**		21:08

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 6 Step(s): 61 Page(s): 40 Date and Time: 30 Nov 2023 21:08 **Note: IW describes the exception(s) and action(s) below.**	AA	2108

Bio Brake for all participants

HSMFD SHA-256 HASH **2023/11/30**

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

 SHA-256:     5c9ad14c8628b3176a841379f9cf1d7c37213a8669b69d6dabecf77292e53c37
PGP Words:  escape newsletter stairway disbelief necklace cellulose scallion bookseller Gei
ger Jupiter Aztec inertia waffle Saturday Belfast informant clamshell Camelot cleanup lette
rhead gazelle potato quadrant hazardous rhythm unicorn virus holiness physique travesty cob
ra consensus
```

```
Script started on 2023-11-30 19:00:48+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=0.906 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.758 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.700 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.730 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.700/0.773/0.906/0.079 ms
\033[?2004h(kskm) root@coen:/media/HSMFD# cd /media/KSRFD/KSK51/
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# kskm-ksrsigner
2023-11-30 19:20:47,561: kskm.common.config: INFO Loaded configuration from file ksrsigner.yaml SHA-256 0f716d1970db983479735e132e858eeea2dae3e250f0cecca41335e94cd43350 WORDS artist hideaway goggles bottomless guidance suspicious printer confidence jawbone hurricane eyeglass barbecue buzzard leprosy orca universe rebirth surrender tissue tomorrow drumbeat upcoming spyglass revolver regain barbecue chopper ultimate drainage souvenir chisel embezzle
2023-11-30 19:20:47,602: kskm.common.config: INFO Configuration validated
2023-11-30 19:20:47,603: kskm.skr.load: INFO Loaded SKR from file skr-root-2023-q4-0.xml SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9ff119e6cc5aed49 WORDS klaxon intention Neptune Virginia skullcap pharmacy ammo hesitate uproot getaway retouch inventive trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getaway uneartH existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
2023-11-30 19:20:47,844: kskm.tools.ksrsigner: INFO Previous SKR:
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO #  Inception           Expiration           ZSK Tags      KSK(CKA_LABEL)
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 1  2023-10-01T00:00:00 2023-10-22T00:00:00  11019,46780   20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 2  2023-10-11T00:00:00 2023-11-01T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 3  2023-10-21T00:00:00 2023-11-11T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 4  2023-10-31T00:00:00 2023-11-21T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 5  2023-11-10T00:00:00 2023-12-01T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 6  2023-11-20T00:00:00 2023-12-11T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 7  2023-11-30T00:00:00 2023-12-21T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 8  2023-12-10T00:00:00 2023-12-31T00:00:00  46780         20326(Klajeyz)/S
2023-11-30 19:20:47,845: kskm.tools.ksrsigner: INFO 9  2023-12-20T00:00:00 2024-01-10T00:00:00  30903,46780   20326(Klajeyz)/S
2023-11-30 19:20:47,846: kskm.ksr.load: INFO Loaded KSR from file ksr-root-2024-q1-0.xml SHA-256 d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5 WORDS stapler businessman prefer unicorn breadline specialist breakup gossamer cranky pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist amusement crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visitor
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO Validating KSR using request policy:
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   _dataclass_placeholder: None
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   acceptable_domains: ['.']
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   approved_algorithms: ['RSASHA256']
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_bundle_intervals: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_bundle_overlap: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_chain_keys: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_chain_keys_in_hsm: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_chain_overlap: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_cycle_length: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_keys_match_ksk_operator_policy: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_keys_publish_safety: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   check_keys_retire_safety: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   dns_ttl: 172800
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   enable_unsupported_ecdsa: False
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   keys_match_zsk_policy: True
2023-11-30 19:20:47,849: kskm.ksr.validate: INFO   max_bundle_interval: 11 days, 0:00:00
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   max_cycle_inception_length: 81 days, 0:00:00
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   min_bundle_interval: 9 days, 0:00:00
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   min_cycle_inception_length: 79 days, 0:00:00
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   num_bundles: 9
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   num_different_keys_in_all_bundles: 3
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   num_keys_per_bundle: [2, 1, 1, 1, 1, 1, 1, 1, 2]
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   rsa_approved_exponents: [65537]
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   rsa_approved_key_sizes: [2048]
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   rsa_exponent_match_zsk_policy: True
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   signature_algorithms_match_zsk_policy: True
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   signature_check_expire_horizon: True
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   signature_horizon_days: 180
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   signature_validity_match_zsk_policy: True
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO   validate_signatures: True
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO KSR-DOMAIN: Verified domain '.'
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO KSR-ID: Will be checked later, when SKR is available
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO KSR-BUNDLE-UNIQUE: All 9 bundles have unique ids
2023-11-30 19:20:47,850: kskm.ksr.validate: INFO KSR-BUNDLE-KEYS: All 3 unique keys in the bundles accepted by policy
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-BUNDLE-POP: All 9 bundles contain proof-of-possession
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-BUNDLE-COUNT: Number of bundles (9) accepted
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-BUNDLE-CYCLE-DURATION: The cycle length is in accordance with the KSK operator policy
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-POLICY-KEYS: Validated number of keys per bundle, and for all bundles
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-POLICY-ALG: All 1 ZSK operator signature algorithms accepted by policy
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-POLICY-SIG-OVERLAP: All bundles overlap in accordance with the stated ZSK operator policy
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-POLICY-SIG-VALIDITY: All 9 bundles have 21 days <= validity >= 21 days
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-POLICY-SIG-HORIZON: All signatures expire in less than 180 days
2023-11-30 19:20:47,852: kskm.ksr.validate: INFO KSR-POLICY-BUNDLE-INTERVALS: All bundles intervals in accordance with the KSK operator policy
2023-11-30 19:20:47,852: kskm.tools.ksrsigner: INFO Request:
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO #  Inception           Expiration           ZSK Tags      KSK(CKA_LABEL)
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 1  2024-01-01T00:00:00 2024-01-22T00:00:00  30903,46780
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 2  2024-01-11T00:00:00 2024-02-01T00:00:00  30903
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 3  2024-01-21T00:00:00 2024-02-11T00:00:00  30903
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 4  2024-01-31T00:00:00 2024-02-21T00:00:00  30903
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 5  2024-02-10T00:00:00 2024-03-02T00:00:00  30903
```

```
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 6  2024-02-20T00:00:00 2024-03-12T00:
00:00  30903
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 7  2024-03-01T00:00:00 2024-03-22T00:
00:00  30903
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 8  2024-03-11T00:00:00 2024-04-01T00:
00:00  30903
2023-11-30 19:20:47,853: kskm.tools.ksrsigner: INFO 9  2024-03-21T00:00:00 2024-04-11T00:
00:00  5613,30903
2023-11-30 19:20:47,853: 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
2023-11-30 19:20:48,078: kskm.misc.hsm: INFO HSM First slot:       ICANNKSK

2023-11-30 19:20:48,078: kskm.misc.hsm: INFO HSM ManufacturerID:  Ultra Electronics AEP N
etworks
2023-11-30 19:20:48,078: kskm.misc.hsm: INFO HSM Model:           Keyper 9860-2
2023-11-30 19:20:48,078: kskm.misc.hsm: INFO HSM Serial:          H1903018
2023-11-30 19:20:48,078: kskm.signer.verify_chain: INFO Checking coherence between SKR(n-
1) and this KSR
2023-11-30 19:20:48,078: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: The last keys in
SKR(n-1) matches the first keys in this KSR
2023-11-30 19:20:48,079: 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
2023-11-30 19:20:48,079: 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-2024-q1-0.xml
SHA-256 HEX:    d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5
SHA-256 WORDS:  stapler businessman prefer unicorn breadline specialist breakup gossamer
cranky pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit
graduate enlist amusement crackdown component skydive Jamaica rhythm millionaire guidance
 cannonball brickyard visitor

Sign KSR? Confirm with "Yes" (exactly) or anything else to abort: Yes
2023-11-30 19:24:02,048: kskm.signer.policy: INFO KSR-POLICY-SAFETY: PublishSafety valida
ted
2023-11-30 19:24:02,049: kskm.signer.policy: INFO KSR-POLICY-SAFETY: RetireSafety validat
ed
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO Generated SKR:
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO #  Inception           Expiration
       ZSK Tags      KSK(CKA_LABEL)
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 1  2024-01-01T00:00:00 2024-01-22T00:
00:00  30903,46780   20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 2  2024-01-11T00:00:00 2024-02-01T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 3  2024-01-21T00:00:00 2024-02-11T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 4  2024-01-31T00:00:00 2024-02-21T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 5  2024-02-10T00:00:00 2024-03-02T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 6  2024-02-20T00:00:00 2024-03-12T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 7  2024-03-01T00:00:00 2024-03-22T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 8  2024-03-11T00:00:00 2024-04-01T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 19:24:02,049: kskm.tools.ksrsigner: INFO 9  2024-03-21T00:00:00 2024-04-11T00:
00:00  30903,5613    20326(Klajeyz)/S
2023-11-30 19:24:02,178: kskm.signer: INFO Wrote SKR to file skr-root-2024-q1-0.xml SHA-2
56 0f2922c76d8ac758dedff603d0c2e44e13369c1938d56ef7509425abf8f0b48f WORDS artist certify
blockade retraction goggles maverick soybean everyday tactics therapist village aggregate
 stagnate repellent tonic distortion Aztec congregate python bottomless classic specialis
t goldfish voyager drumbeat molecule bombast Pegasus Vulcan upcoming scenic midsummer
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# printlog kskm-ksrsigner-20231130-192047-8
94.log
[023 1 copy ] sent to printer
6 lines were wrapped
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# printlog kskm-ksrsigner-20231130-192047-8
94.log
[023 1 copy ] sent to printer
6 lines were wrapped
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# 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/KSRFD/KSK51# head -c 375431168 /dev/sda | sha2wordlist
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/KSRFD/KSK51# ping hsm
PING hsm (192.168.0.2) 56(84) bytes of data.
64 bytes from hsm (192.168.0.2): icmp_seq=1 ttl=255 time=0.924 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.583 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.727 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.743 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3030ms
rtt min/avg/max/mdev = 0.583/0.744/0.924/0.121 ms
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# cd HSM7E/
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# kskm-ksrsigner
2023-11-30 20:17:30,875: kskm.common.config: INFO Loaded configuration from file ksrsigne
r.yaml SHA-256 432a513b007acc8ae97057bccefca01f36dd334d00e7cac0462df3abc3a69388 WORDS cru
cial chambermaid drunken councilman aardvark infancy spigot maverick treadmill hesitate e
ightball pyramid spyglass Wilmington ragtime businessman Christmas tambourine chisel disr
uptive aardvark truncated spellbind recipe cubic clergyman upset Pegasus snowcap paragon
playhouse maritime
2023-11-30 20:17:30,915: kskm.common.config: INFO Configuration validated
2023-11-30 20:17:30,916: kskm.skr.load: INFO Loaded SKR from file skr-root-2023-q4-0.xml
SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9ff119e6cc5aed49 WORDS klaxon int
ention Neptune Virginia skullcap pharmacy ammo hesitate uproot getaway retouch inventive
trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getaway uneart
h existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO Previous SKR:
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO #  Inception           Expiration
       ZSK Tags      KSK(CKA_LABEL)
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO 1  2023-10-01T00:00:00 2023-10-22T00:
00:00  46780,11019   20326(Klajeyz)/S
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO 2  2023-10-11T00:00:00 2023-11-01T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO 3  2023-10-21T00:00:00 2023-11-11T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO 4  2023-10-31T00:00:00 2023-11-21T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,954: kskm.tools.ksrsigner: INFO 5  2023-11-10T00:00:00 2023-12-01T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,955: kskm.tools.ksrsigner: INFO 6  2023-11-20T00:00:00 2023-12-11T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,955: kskm.tools.ksrsigner: INFO 7  2023-11-30T00:00:00 2023-12-21T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,955: kskm.tools.ksrsigner: INFO 8  2023-12-10T00:00:00 2023-12-31T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:17:30,955: kskm.tools.ksrsigner: INFO 9  2023-12-20T00:00:00 2024-01-10T00:
00:00  46780,30903   20326(Klajeyz)/S
2023-11-30 20:17:30,956: kskm.ksr.load: INFO Loaded KSR from file ksr-root-2024-q1-0.xml
SHA-256 d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5 WORDS stapler bu
sinessman prefer unicorn breadline specialist breakup gossamer cranky pedigree stapler py
```

```
ramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist amusement
crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visi
tor
2023-11-30 20:17:30,958: kskm.ksr.validate: INFO Validating KSR using request policy:
2023-11-30 20:17:30,958: kskm.ksr.validate: INFO   _dataclass_placeholder: None
2023-11-30 20:17:30,958: kskm.ksr.validate: INFO   acceptable_domains: ['.']
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   approved_algorithms: ['RSASHA256']
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_bundle_intervals: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_bundle_overlap: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_chain_keys: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_chain_keys_in_hsm: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_chain_overlap: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_cycle_length: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_keys_match_ksk_operator_policy:
True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_keys_publish_safety: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   check_keys_retire_safety: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   dns_ttl: 172800
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   enable_unsupported_ecdsa: False
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   keys_match_zsk_policy: True
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   max_bundle_interval: 11 days, 0:00:00
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   max_cycle_inception_length: 81 days, 0
:00:00
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   min_bundle_interval: 9 days, 0:00:00
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   min_cycle_inception_length: 79 days, 0
:00:00
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   num_bundles: 9
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   num_different_keys_in_all_bundles: 3
2023-11-30 20:17:30,959: kskm.ksr.validate: INFO   num_keys_per_bundle: [2, 1, 1, 1, 1, 1
, 1, 1, 2]
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   rsa_approved_exponents: [65537]
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   rsa_approved_key_sizes: [2048]
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   rsa_exponent_match_zsk_policy: True
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   signature_algorithms_match_zsk_policy:
 True
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   signature_check_expire_horizon: True
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   signature_horizon_days: 180
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   signature_validity_match_zsk_policy: T
rue
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO   validate_signatures: True
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO KSR-DOMAIN: Verified domain '.'
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO KSR-ID: Will be checked later, when SKR
is available
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO KSR-BUNDLE-UNIQUE: All 9 bundles have un
ique ids
2023-11-30 20:17:30,960: kskm.ksr.validate: INFO KSR-BUNDLE-KEYS: All 3 unique keys in th
e bundles accepted by policy
2023-11-30 20:17:30,961: kskm.ksr.validate: INFO KSR-BUNDLE-POP: All 9 bundles contain pr
oof-of-possession
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-BUNDLE-COUNT: Number of bundles (9)
accepted
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-BUNDLE-CYCLE-DURATION: The cycle len
gth is in accordance with the KSK operator policy
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-POLICY-KEYS: Validated number of key
s per bundle, and for all bundles
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-POLICY-ALG: All 1 ZSK operator signa
ture algorithms accepted by policy
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-POLICY-SIG-OVERLAP: All bundles over
lap in accordance with the stated ZSK operator policy
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-POLICY-SIG-VALIDITY: All 9 bundles h
ave 21 days <= validity >= 21 days
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-POLICY-SIG-HORIZON: All signatures e
xpire in less than 180 days
2023-11-30 20:17:30,962: kskm.ksr.validate: INFO KSR-POLICY-BUNDLE-INTERVALS: All bundles
 intervals in accordance with the KSK operator policy
2023-11-30 20:17:30,962: kskm.tools.ksrsigner: INFO Request:
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO #  Inception           Expiration
      ZSK Tags      KSK(CKA_LABEL)
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 1  2024-01-01T00:00:00 2024-01-22T00:
00:00  46780,30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 2  2024-01-11T00:00:00 2024-02-01T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 3  2024-01-21T00:00:00 2024-02-11T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 4  2024-01-31T00:00:00 2024-02-21T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 5  2024-02-10T00:00:00 2024-03-02T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 6  2024-02-20T00:00:00 2024-03-12T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 7  2024-03-01T00:00:00 2024-03-22T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 8  2024-03-11T00:00:00 2024-04-01T00:
00:00  30903
2023-11-30 20:17:30,963: kskm.tools.ksrsigner: INFO 9  2024-03-21T00:00:00 2024-04-11T00:
00:00  5613,30903
2023-11-30 20:17:30,963: 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
2023-11-30 20:17:31,126: kskm.misc.hsm: INFO HSM First slot:       ICANNKSK

2023-11-30 20:17:31,126: kskm.misc.hsm: INFO HSM ManufacturerID:  Ultra Electronics AEP N
etworks
2023-11-30 20:17:31,126: kskm.misc.hsm: INFO HSM Model:           Keyper 9860-2
2023-11-30 20:17:31,126: kskm.misc.hsm: INFO HSM Serial:          H2110009
2023-11-30 20:17:31,127: kskm.signer.verify_chain: INFO Checking coherence between SKR(n-
1) and this KSR
2023-11-30 20:17:31,127: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: The last keys in
SKR(n-1) matches the first keys in this KSR
2023-11-30 20:17:31,127: 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
2023-11-30 20:17:31,128: 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-2024-q1-0.xml
SHA-256 HEX:    d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5
SHA-256 WORDS:  stapler businessman prefer unicorn breadline specialist breakup gossamer
cranky pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit
graduate enlist amusement crackdown component skydive Jamaica rhythm millionaire guidance
 cannonball brickyard visitor

Sign KSR? Confirm with "Yes" (exactly) or anything else to abort: Yes
2023-11-30 20:19:41,974: kskm.signer.policy: INFO KSR-POLICY-SAFETY: PublishSafety valida
ted
2023-11-30 20:19:41,974: kskm.signer.policy: INFO KSR-POLICY-SAFETY: RetireSafety validat
ed
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO Generated SKR:
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO #  Inception           Expiration
      ZSK Tags      KSK(CKA_LABEL)
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO 1  2024-01-01T00:00:00 2024-01-22T00:
00:00  46780,30903   20326(Klajeyz)/S
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO 2  2024-01-11T00:00:00 2024-02-01T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO 3  2024-01-21T00:00:00 2024-02-11T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO 4  2024-01-31T00:00:00 2024-02-21T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO 5  2024-02-10T00:00:00 2024-03-02T00:
00:00  30903         20326(Klajeyz)/S
```

```
2023-11-30 20:19:41,975: kskm.tools.ksrsigner: INFO 6  2024-02-20T00:00:00 2024-03-12T00:
00:00  30903          20326(Klajeyz)/S
2023-11-30 20:19:41,976: kskm.tools.ksrsigner: INFO 7  2024-03-01T00:00:00 2024-03-22T00:
00:00  30903          20326(Klajeyz)/S
2023-11-30 20:19:41,976: kskm.tools.ksrsigner: INFO 8  2024-03-11T00:00:00 2024-04-01T00:
00:00  30903          20326(Klajeyz)/S
2023-11-30 20:19:41,976: kskm.tools.ksrsigner: INFO 9  2024-03-21T00:00:00 2024-04-11T00:
00:00  5613,30903     20326(Klajeyz)/S
2023-11-30 20:19:42,106: kskm.signer: INFO Wrote SKR to file HSM7E-skr-root-2024-q1-0.xml
 SHA-256 0f2922c76d8ac758dedff603d0c2e44e13369c1938d56ef7509425abf8f0b48f WORDS artist ce
rtify blockade retraction goggles maverick soybean everyday tactics therapist village agg
regate stagnate repellent tonic distortion Aztec congregate python bottomless classic spe
cialist goldfish voyager drumbeat molecule bombast Pegasus Vulcan upcoming scenic midsumm
er
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# printlog kskm-ksrsigner-20231130-20
1730-997.log 7
[ 1 copy ] sent to printer
6 lines were wrapped
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# cat style.xsl
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" indent="yes" omit-xml-declaration="yes"/>
  <xsl:template match="@* | node()">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()"/>
    </xsl:copy>
  </xsl:template>
  <xsl:template match="ResponseBundle">
    <xsl:copy>
      <xsl:apply-templates select="Inception"/>
      <xsl:apply-templates select="Expiration"/>
      <xsl:apply-templates select="Key">
        <xsl:sort select="@keyIdentifier"/>
      </xsl:apply-templates>
      <xsl:apply-templates select="Signature"/>
    </xsl:copy>
  </xsl:template>
</xsl:stylesheet>

\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# xsltproc style.xsl ../skr-\007root-
2024-q1-0.xml | xmllint --f
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# xsltproc style.xsl HSM7E-skr-root-2
024-q1-0.xml | xmllint
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# diff -wu current new
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM7E# cd ..
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# ping hsm
PING 192.168.0.2) 56(84) bytes of data.
64 bytes from hsm (192.168.0.2): icmp_seq=1 ttl=255 time=0.991 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.609 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.714 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.581 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.581/0.723/0.991/0.162 ms
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51# cd HSM8E
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# kskm-ksrsigner
2023-11-30 20:47:16,409: kskm.common.config: INFO Loaded configuration from file ksrsigne
r.yaml SHA-256 393b1acd14c7dbdb975539ada03d4f7ce4822500c460f6f3603a7e4ae4fd20b9 WORDS cla
ssroom councilman beehive sandalwood baboon retraction suspense suspicious preshrunk equi
pment classroom perceptive ragtime crucifix dropper informant tonic Istanbul bombast adro
itness snowslide fortitude village vertigo facial corrosion locale direction tonic Wyomin
g bison proximate
2023-11-30 20:47:16,448: kskm.common.config: INFO Configuration validated
2023-11-30 20:47:16,450: kskm.skr.load: INFO Loaded SKR from file skr-root-2023-q4-0.xml
SHA-256 7d8087f4bdaf0c70f264a881eb07ec16ae15d8fb3764f05a9ff119e6cc5aed49 WORDS klaxon int
ention Neptune Virginia skullcap pharmacy ammo hesitate uproot getaway retouch inventive
trouble amusement tumor bodyguard robust bifocals stormy Wichita clamshell getaway uneart
h existence quota vacancy bedlamp trombonist spigot existence tunnel dinosaur
2023-11-30 20:47:16,487: kskm.tools.ksrsigner: INFO Previous SKR:
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO #  Inception           Expiration
       ZSK Tags      KSK(CKA_LABEL)
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 1  2023-10-01T00:00:00 2023-10-22T00:
00:00  46780,11019   20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 2  2023-10-11T00:00:00 2023-11-01T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 3  2023-10-21T00:00:00 2023-11-11T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 4  2023-10-31T00:00:00 2023-11-21T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 5  2023-11-10T00:00:00 2023-12-01T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 6  2023-11-20T00:00:00 2023-12-11T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 7  2023-11-30T00:00:00 2023-12-21T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 8  2023-12-10T00:00:00 2023-12-31T00:
00:00  46780         20326(Klajeyz)/S
2023-11-30 20:47:16,488: kskm.tools.ksrsigner: INFO 9  2023-12-20T00:00:00 2024-01-10T00:
00:00  46780,30903   20326(Klajeyz)/S
2023-11-30 20:47:16,489: kskm.ksr.load: INFO Loaded KSR from file ksr-root-2024-q1-0.xml
SHA-256 d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5 WORDS stapler bu
sinessman prefer unicorn breadline specialist breakup gossamer cranky pedigree stapler py
ramid tunnel forever tumor congregate indulge Waterloo transit graduate enlist amusement
crackdown component skydive Jamaica rhythm millionaire guidance cannonball brickyard visi
tor
2023-11-30 20:47:16,491: kskm.ksr.validate: INFO Validating KSR using request policy:
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   _dataclass_placeholder: None
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   acceptable_domains: ['.']
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   approved_algorithms: ['RSASHA256']
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_bundle_intervals: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_bundle_overlap: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_chain_keys: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_chain_keys_in_hsm: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_chain_overlap: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_cycle_length: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_keys_match_ksk_operator_policy:
True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_keys_publish_safety: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   check_keys_retire_safety: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   dns_ttl: 172800
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   enable_unsupported_ecdsa: False
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   keys_match_zsk_policy: True
2023-11-30 20:47:16,492: kskm.ksr.validate: INFO   max_bundle_interval: 11 days, 0:00:00
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   max_cycle_inception_length: 81 days, 0
:00:00
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   min_bundle_interval: 9 days, 0:00:00
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   min_cycle_inception_length: 79 days, 0
:00:00
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   num_bundles: 9
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   num_different_keys_in_all_bundles: 3
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   num_keys_per_bundle: [2, 1, 1, 1, 1, 1
, 1, 1, 2]
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   rsa_approved_exponents: [65537]
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   rsa_approved_key_sizes: [2048]
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   rsa_exponent_match_zsk_policy: True
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   signature_algorithms_match_zsk_policy:
 True
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   signature_check_expire_horizon: True
```

```
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   signature_horizon_days: 180
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   signature_validity_match_zsk_policy: T
rue
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO   validate_signatures: True
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO KSR-DOMAIN: Verified domain '.'
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO KSR-ID: Will be checked later, when SKR
is available
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO KSR-BUNDLE-UNIQUE: All 9 bundles have un
ique ids
2023-11-30 20:47:16,493: kskm.ksr.validate: INFO KSR-BUNDLE-KEYS: All 3 unique keys in th
e bundles accepted by policy
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-BUNDLE-POP: All 9 bundles contain pr
oof-of-possession
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-BUNDLE-COUNT: Number of bundles (9)
accepted
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-BUNDLE-CYCLE-DURATION: The cycle len
gth is in accordance with the KSK operator policy
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-POLICY-KEYS: Validated number of key
s per bundle, and for all bundles
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-POLICY-ALG: All 1 ZSK operator signa
ture algorithms accepted by policy
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-POLICY-SIG-OVERLAP: All bundles over
lap in accordance with the stated ZSK operator policy
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-POLICY-SIG-VALIDITY: All 9 bundles h
ave 21 days <= validity >= 21 days
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-POLICY-SIG-HORIZON: All signatures e
xpire in less than 180 days
2023-11-30 20:47:16,495: kskm.ksr.validate: INFO KSR-POLICY-BUNDLE-INTERVALS: All bundles
 intervals in accordance with the KSK operator policy
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO Request:
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO #  Inception           Expiration
      ZSK Tags      KSK(CKA_LABEL)
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 1  2024-01-01T00:00:00 2024-01-22T00:
00:00  46780,30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 2  2024-01-11T00:00:00 2024-02-01T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 3  2024-01-21T00:00:00 2024-02-11T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 4  2024-01-31T00:00:00 2024-02-21T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 5  2024-02-10T00:00:00 2024-03-02T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 6  2024-02-20T00:00:00 2024-03-12T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 7  2024-03-01T00:00:00 2024-03-22T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 8  2024-03-11T00:00:00 2024-04-01T00:
00:00  30903
2023-11-30 20:47:16,496: kskm.tools.ksrsigner: INFO 9  2024-03-21T00:00:00 2024-04-11T00:
00:00  30903,5613
2023-11-30 20:47:16,496: 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
2023-11-30 20:47:16,666: kskm.misc.hsm: INFO HSM First slot:       ICANNKSK

2023-11-30 20:47:16,666: kskm.misc.hsm: INFO HSM ManufacturerID:  Ultra Electronics AEP N
etworks
2023-11-30 20:47:16,666: kskm.misc.hsm: INFO HSM Model:           Keyper 9860-2
2023-11-30 20:47:16,666: kskm.misc.hsm: INFO HSM Serial:          H2110010
2023-11-30 20:47:16,666: kskm.signer.verify_chain: INFO Checking coherence between SKR(n-
1) and this KSR
2023-11-30 20:47:16,667: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: The last keys in
SKR(n-1) matches the first keys in this KSR
2023-11-30 20:47:16,667: 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
2023-11-30 20:47:16,668: 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-2024-q1-0.xml
SHA-256 HEX:    d31f96ec28d5296641aad3bced5fec3675f9e7675a074032be83ab9070232af5
SHA-256 WORDS:  stapler businessman prefer unicorn breadline specialist breakup gossamer
cranky pedigree stapler pyramid tunnel forever tumor congregate indulge Waterloo transit
graduate enlist amusement crackdown component skydive Jamaica rhythm millionaire guidance
 cannonball brickyard visitor

Sign KSR? Confirm with "Yes" (exactly) or anything else to abort: Yes
2023-11-30 20:48:41,774: kskm.signer.policy: INFO KSR-POLICY-SAFETY: PublishSafety valida
ted
2023-11-30 20:48:41,774: kskm.signer.policy: INFO KSR-POLICY-SAFETY: RetireSafety validat
ed
2023-11-30 20:48:41,774: kskm.tools.ksrsigner: INFO Generated SKR:
2023-11-30 20:48:41,774: kskm.tools.ksrsigner: INFO #  Inception           Expiration
      ZSK Tags      KSK(CKA_LABEL)
2023-11-30 20:48:41,774: kskm.tools.ksrsigner: INFO 1  2024-01-01T00:00:00 2024-01-22T00:
00:00  46780,30903   20326(Klajeyz)/S
2023-11-30 20:48:41,774: kskm.tools.ksrsigner: INFO 2  2024-01-11T00:00:00 2024-02-01T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 3  2024-01-21T00:00:00 2024-02-11T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 4  2024-01-31T00:00:00 2024-02-21T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 5  2024-02-10T00:00:00 2024-03-02T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 6  2024-02-20T00:00:00 2024-03-12T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 7  2024-03-01T00:00:00 2024-03-22T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 8  2024-03-11T00:00:00 2024-04-01T00:
00:00  30903         20326(Klajeyz)/S
2023-11-30 20:48:41,775: kskm.tools.ksrsigner: INFO 9  2024-03-21T00:00:00 2024-04-11T00:
00:00  30903,5613    20326(Klajeyz)/S
2023-11-30 20:48:41,902: kskm.signer: INFO Wrote SKR to file HSM8E-skr-root-2024-q1-0.xml
 SHA-256 0f2922c76d8ac758dedff603d0c2e44e13369c1938d56ef7509425abf8f0b48f WORDS artist ce
rtify blockade retraction goggles maverick soybean everyday tactics therapist village agg
regate stagnate repellent tonic distortion Aztec congregate python bottomless classic spe
cialist goldfish voyager drumbeat molecule bombast Pegasus Vulcan upcoming scenic midsumm
er
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# printlog kskm-ksrsigner-20231130-20
4716-1058.log 8
[023 [ 1 copy ] sent to printer
6 lines were wrapped
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# cat style.xsl
<?xml version="1.0"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" indent="yes" omit-xml-declaration="yes"/>
  <xsl:template match="@* | node()">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()"/>
    </xsl:copy>
  </xsl:template>
  <xsl:template match="ResponseBundle">
    <xsl:copy>
      <xsl:apply-templates select="Inception"/>
      <xsl:apply-templates select="Expiration"/>
      <xsl:apply-templates select="Key">
        <xsl:sort select="@keyIdentifier"/>
      </xsl:apply-templates>
      <xsl:apply-templates select="Signature"/>
    </xsl:copy>
  </xsl:template>
```

```
</xsl:stylesheet>

\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# xsltproc style.xsl /./sk\007r-root-
2024-q1-0.xml > new
\033[?2004l
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# xsltproc style.xsl HSM8E-skr-root-2
024-q1-0.xml > new
\033[?2004l
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# diff -wu current new
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK51/HSM8E# cd /media/HSMFD/
\033[?2004h(kskm) root@coen:/media/HSMFD# ls -ltrR /media/KSRFD/
/media/KSRFD/:
total 16
drwxr-xr-x 4 root root 16384 Nov 30 19:24 \033[0m\033[01;34mKSK51\033[0m

/media/KSRFD/KSK51:
total 160
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11501 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 24832 Nov 30 19:24 skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11079 Nov 30 19:24 kskm-ksrsigner-20231130-192047-894.log
drwxr-xr-x 2 root root 16384 Nov 30 20:23 \033[01;34mHSM7E\033[0m
drwxr-xr-x 2 root root 16384 Nov 30 20:51 \033[01;34mHSM8E\033[0m

/media/KSRFD/KSK51/HSM7E:
total 208
-rw-r--r-- 1 root root   652 Nov 17 22:23 style.xsl
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11507 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 24832 Nov 30 20:19 HSM7E-skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11097 Nov 30 20:19 kskm-ksrsigner-20231130-201730-997.log
-rw-r--r-- 1 root root 22205 Nov 30 20:23 current
-rw-r--r-- 1 root root 22205 Nov 30 20:23 new

/media/KSRFD/KSK51/HSM8E:
total 208
-rw-r--r-- 1 root root   652 Nov 17 22:23 style.xsl
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11507 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11096 Nov 30 20:48 kskm-ksrsigner-20231130-204716-1058.log
-rw-r--r-- 1 root root 24832 Nov 30 20:48 HSM8E-skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 22205 Nov 30 20:51 current
-rw-r--r-- 1 root root 22205 Nov 30 20:51 new
\033[?2004h(kskm) root@coen:/media/HSMFD# cp /media/KSRFD/* .
\033[?2004h(kskm) root@coen:/media/HSMFD# ls -ltrR
\033[?2004l
total 3400
-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   7674 Jun 16  2010 script-20100616-2209utc.log
-rw-r--r-- 1 root root  18364 Oct 31  2010 skr.xml.20101101181303
-rw-r--r-- 1 root root  15547 Oct 31  2010 ksr-root-2011-q1-0.xml
-rw-r--r-- 1 root root  18402 Nov  1  2010 skr-root-2011-q1-0.xml
-rw-r--r-- 1 root root   5504 Nov  1  2010 ksrsigner-20101101-181303.log
-rw-r--r-- 1 root root  14005 Nov  1  2010 ttyaudit-ttyUSB0-20101101-175457.log
-rw-r--r-- 1 root root   7161 Nov  1  2010 script-20101101.log
-rw-r--r-- 1 root root  18402 Feb  7  2011 skr.xml.20110511181632
-rw-r--r-- 1 root root  15547 Apr 25  2011 ksr-root-2011-q3-0.xml
-rw-r--r-- 1 root root   1400 May 11  2011 ksrsigner-20110511-181351.log
-rw-r--r-- 1 root root  18402 May 11  2011 skr-root-2011-q3-0.xml
-rw-r--r-- 1 root root   5510 May 11  2011 ksrsigner-20110511-181632.log
-rw-r--r-- 1 root root  14374 May 11  2011 ttyaudit-ttyUSB0-20110511-180559.log
-rw-r--r-- 1 root root   9133 May 11  2011 script-20110511.log
-rw-r--r-- 1 root root  18404 Jul 20  2011 skr.xml.20110930181607
-rw-r--r-- 1 root root  15587 Sep 23  2011 ksr-root-2012-q1-0.xml
-rw-r--r-- 1 root root  18422 Sep 30  2011 skr-root-2012-q1-0.xml
-rw-r--r-- 1 root root   5609 Sep 30  2011 ksrsigner-20110930-181607.log
-rw-r--r-- 1 root root  12034 Sep 30  2011 ttyaudit-ttyUSB0-20110930-180703.log
-rw-r--r-- 1 root root   7270 Sep 30  2011 script-20110930.log
-rw-r--r-- 1 root root  18424 Feb  2  2012 skr.xml.20120522151741
-rw-r--r-- 1 root root  15571 May  9  2012 ksr-root-2012-q3-0.xml
-rw-r--r-- 1 root root  18414 May 22  2012 skr-root-2012-q3-0.xml
-rw-r--r-- 1 root root   5528 May 22  2012 ksrsigner-20120522-151741.log
-rw-r--r-- 1 root root  12034 May 22  2012 ttyaudit-ttyUSB0-20120522-150621.log
-rw-r--r-- 1 root root  13817 May 22  2012 script-20120522.log
-rw-r--r-- 1 root root  18324 Jul 26  2012 skr.xml.20121112155152
-rw-r--r-- 1 root root  15371 Oct 12  2012 ksr-root-2013-q1-0.xml
-rw-r--r-- 1 root root  18314 Nov 12  2012 skr-root-2013-q1-0.xml
-rw-r--r-- 1 root root   5529 Nov 12  2012 ksrsigner-20121112-155152.log
-rw-r--r-- 1 root root  12044 Nov 12  2012 ttyaudit-ttyUSB0-20121112-154229.log
-rw-r--r-- 1 root root  12249 Nov 12  2012 script-20121112.log
-rw-r--r-- 1 root root  18314 Feb 12  2013 skr.xml.20130502190633
-rw-r--r-- 1 root root  15371 Apr  5  2013 ksr-root-2013-q3-0.xml
-rw-r--r-- 1 root root   4004 May  2  2013 ksrsigner-20130502-190252.log
-rw-r--r-- 1 root root  18314 May  2  2013 skr-root-2013-q3-0.xml
-rw-r--r-- 1 root root   5502 May  2  2013 ksrsigner-20130502-190633.log
-rw-r--r-- 1 root root  12397 May  2  2013 ttyaudit-ttyUSB0-20130502-185222.log
-rw-r--r-- 1 root root  21494 May  2  2013 script-20130502.log
-rw-r--r-- 1 root root  18314 Aug  7  2013 skr.xml.20131024184618
-rw-r--r-- 1 root root  15371 Oct  4  2013 ksr-root-2014-q1-0.xml
-rw-r--r-- 1 root root  18314 Oct 24  2013 skr-root-2014-q1-0.xml
-rw-r--r-- 1 root root   5512 Oct 24  2013 ksrsigner-20131024-184618.log
-rw-r--r-- 1 root root  12044 Oct 24  2013 ttyaudit-ttyUSB0-20131024-182843.log
-rw-r--r-- 1 root root   9167 Oct 24  2013 script-20131024.log
-rw-r--r-- 1 root root  18314 Feb 13  2014 skr.xml.20140417183604
-rw-r--r-- 1 root root  15353 Apr  3  2014 ksr-root-2014-q3-0.xml
-rw-r--r-- 1 root root  18314 Apr 17  2014 skr-root-2014-q3-0.xml
-rw-r--r-- 1 root root   5511 Apr 17  2014 ksrsigner-20140417-183604.log
-rw-r--r-- 1 root root  12034 Apr 17  2014 ttyaudit-ttyUSB0-20140417-182117.log
-rw-r--r-- 1 root root   5853 Apr 17  2014 script-20140417.log
-rw-r--r-- 1 root root  18314 Nov 10  2014 skr.xml.20141120201132
-rw-r--r-- 1 root root  15371 Nov 10  2014 ksr-root-2015-q1-0.xml
-rw-r--r-- 1 root root  18314 Nov 20  2014 skr-root-2015-q1-0.xml
-rw-r--r-- 1 root root   5490 Nov 20  2014 ksrsigner-20141120-201132.log
-rw-r--r-- 1 root root  12042 Nov 20  2014 ttyaudit-ttyUSB0-20141120-200407.log
-rw-r--r-- 1 root root   5462 Nov 20  2014 script-20141120-1.log
-rw-r--r-- 1 root root  15353 Apr  1  2015 ksr-root-2015-q3-0.xml
-rw-r--r-- 1 root root  18314 Apr  1  2015 skr.xml.20150409183038
-rw-r--r-- 1 root root  18314 Apr  9  2015 skr-root-2015-q3-0.xml
-rw-r--r-- 1 root root   5621 Apr  9  2015 ksrsigner-20150409-183038.log
-rw-r--r-- 1 root root  15774 Apr  9  2015 ttyaudit-ttyUSB0-20150409-180743.log
-rw-r--r-- 1 root root   5636 Apr  9  2015 ksrsigner-20150409-193635.log
-rw-r--r-- 1 root root  33966 Apr  9  2015 ttyaudit-ttyUSB0-20150409-190117.log
-rw-r--r-- 1 root root   5636 Apr  9  2015 ksrsigner-20150409-205227.log
-rw-r--r-- 1 root root  34895 Apr  9  2015 ttyaudit-ttyUSB0-20150409-202837.log
-rw-r--r-- 1 root root  19175 Apr  9  2015 script-20150409.log
-rw-r--r-- 1 root root  18314 Nov  4  2015 skr.xml.20151112193232
-rw-r--r-- 1 root root  15371 Nov  4  2015 ksr-root-2016-q1-0.xml
-rw-r--r-- 1 root root  18314 Nov 12  2015 skr-root-2016-q1-0.xml
```

```
-rw-r--r-- 1 root root   5547 Nov 12  2015 ksrsigner-20151112-193232.log
-rw-r--r-- 1 root root  12215 Nov 12  2015 ttyaudit-ttyUSB0-20151112-191111.log
-rw-r--r-- 1 root root   7282 Nov 12  2015 script-20151112.log
-rw-r--r-- 1 root root  18314 Apr 29  2016 skr.xml.20160512192325
-rw-r--r-- 1 root root  14301 Apr 29  2016 ksr-root-2016-q3-fallback-1.xml
-rw-r--r-- 1 root root  18314 Apr 29  2016 skr.xml.20160512190619
-rw-r--r-- 1 root root  15994 Apr 29  2016 ksr-root-2016-q3-0.xml
-rw-r--r-- 1 root root  18599 May 12  2016 skr-root-2016-q3-0.xml
-rw-r--r-- 1 root root   5534 May 12  2016 ksrsigner-20160512-190619.log
-rw-r--r-- 1 root root  17908 May 12  2016 skr-root-2016-q3-fallback-1.xml
-rw-r--r-- 1 root root   5566 May 12  2016 ksrsigner-20160512-192325.log
-rw-r--r-- 1 root root  12484 May 12  2016 ttyaudit-ttyUSB0-20160512-184752.log
-rw-r--r-- 1 root root  15870 May 12  2016 script-20160512.log
-rw-r--r-- 1 root root  19557 Oct 24  2016 ksr-root-2017-q1-0.xml
-rw-r--r-- 1 root root  21083 Oct 24  2016 skr.xml.20161027183803
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr.xml
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr-root-2017-q1-0.xml
-rw-r--r-- 1 root root   5501 Oct 27  2016 ksrsigner-20161027-183803.log
-rw-r--r-- 1 root root   2712 Oct 27  2016 kskgen-20161027-184920.log
-rw-r--r-- 1 root root    817 Oct 27  2016 Klajeyz.csr
-rw-r--r-- 1 root root    357 Oct 27  2016 keybackup-20161027-185705.log
-rw-r--r-- 1 root root    357 Oct 27  2016 keybackup-20161027-200501.log
-rw-r--r-- 1 root root  28791 Oct 27  2016 ttyaudit-ttyUSB0-20161027-182428.log
-rw-r--r-- 1 root root  33568 Oct 27  2016 ttyaudit-ttyUSB0-20161027-202240.log
-rw-r--r-- 1 root root  17803 Oct 27  2016 script-20161027.log
-rw-r--r-- 1 root root   6505 Apr 27  2017 ksrsigner-20170427-183853.log
drwxr-xr-x 2 root root   8192 Apr 27  2017 \033[0m\033[01;34mKSK29-0-C_to_D\033[0m
-rw-r--r-- 1 root root   6228 Apr 27  2017 ksrsigner-20170427-184519.log
drwxr-xr-x 2 root root   8192 Apr 27  2017 \033[01;34mKSK29-1-D_to_C\033[0m
-rw-r--r-- 1 root root   6224 Apr 27  2017 ksrsigner-20170427-184912.log
drwxr-xr-x 2 root root   8192 Apr 27  2017 \033[01;34mKSK29-2-C_to_C\033[0m
-rw-r--r-- 1 root root  12913 Apr 27  2017 ttyaudit-ttyUSB0-20170427-182024.log
-rw-r--r-- 1 root root  16683 Apr 27  2017 script-20170427.log
-rw-r--r-- 1 root root      0 Oct 18  2017 script-20171018.log
-rw-r--r-- 1 root root   8192 Oct 18  2017 ttyaudit-ttyUSB0-20171018-174745.log
-rw-r--r-- 1 root root   6681 Oct 18  2017 ksrsigner-20171018-181941.log
drwxr-xr-x 2 root root   8192 Oct 18  2017 \033[01;34mKSK31-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6698 Oct 18  2017 ksrsigner-20171018-182803.log
drwxr-xr-x 2 root root   8192 Oct 18  2017 \033[01;34mKSK31-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6678 Oct 18  2017 ksrsigner-20171018-183150.log
drwxr-xr-x 2 root root   8192 Oct 18  2017 \033[01;34mKSK31-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6361 Oct 18  2017 ksrsigner-20171018-183453.log
drwxr-xr-x 2 root root   8192 Oct 18  2017 \033[01;34mKSK31-3-C_to_C\033[0m
-rw-r--r-- 1 root root   4384 Oct 18  2017 ttyaudit-ttyUSB0-20171018-175253.log
-rw-r--r-- 1 root root  23163 Oct 18  2017 script-20171018-v2.log
-rw-r--r-- 1 root root  10002 Apr 11  2018 ttyaudit-ttyUSB0-20180411-181102.log
-rw-r--r-- 1 root root   6775 Apr 11  2018 ksrsigner-20180411-183203.log
drwxr-xr-x 2 root root   8192 Apr 11  2018 \033[01;34mKSK33-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6783 Apr 11  2018 ksrsigner-20180411-183607.log
drwxr-xr-x 2 root root   8192 Apr 11  2018 \033[01;34mKSK33-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6776 Apr 11  2018 ksrsigner-20180411-183814.log
drwxr-xr-x 2 root root   8192 Apr 11  2018 \033[01;34mKSK33-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6469 Apr 11  2018 ksrsigner-20180411-184001.log
drwxr-xr-x 2 root root   8192 Apr 11  2018 \033[01;34mKSK33-3-C_to_C\033[0m
-rw-r--r-- 1 root root      0 Apr 11  2018 ttyaudit-ttyUSB0-20180411-185854.log
-rw-r--r-- 1 root root  36029 Apr 11  2018 script-20180411.log
-rw-r--r-- 1 root root   6757 Nov 15  2018 ksrsigner-20181115-194236.log
drwxr-xr-x 2 root root   8192 Nov 15  2018 \033[01;34mKSK35-0-E_to_F\033[0m
-rw-r--r-- 1 root root   6449 Nov 15  2018 ksrsigner-20181115-195208.log
drwxr-xr-x 2 root root   8192 Nov 15  2018 \033[01;34mKSK35-1-F_to_G\033[0m
-rw-r--r-- 1 root root   6775 Nov 15  2018 ksrsigner-20181115-195448.log
drwxr-xr-x 2 root root   8192 Nov 15  2018 \033[01;34mKSK35-2-E_to_E\033[0m
-rw-r--r-- 1 root root   6765 Nov 15  2018 ksrsigner-20181115-195652.log
drwxr-xr-x 2 root root   8192 Nov 15  2018 \033[01;34mKSK35-3-D_to_D\033[0m
-rw-r--r-- 1 root root  14444 Nov 15  2018 ttyaudit-ttyS0-20181115-192849.log
-rw-r--r-- 1 root root  39692 Nov 15  2018 script-20181115.log
drwxr-xr-x 2 root root   8192 May 16  2019 \033[01;34mKSK37\033[0m
-rw-r--r-- 1 root root   6271 May 16  2019 ksrsigner-20190516-190831.log
-rw-r--r-- 1 root root    357 May 16  2019 keybackup-20190516-200518.log
-rw-r--r-- 1 root root    210 May 16  2019 keybackup-20190516-200704.log
-rw-r--r-- 1 root root    271 May 16  2019 keybackup-20190516-200726.log
-rw-r--r-- 1 root root   6286 May 16  2019 ksrsigner-20190516-205655.log
-rw-r--r-- 1 root root  92098 May 16  2019 ttyaudit-ttyS0-20190516-185410.log
-rw-r--r-- 1 root root  30612 May 16  2019 script-20190516.log
-rw-r--r-- 1 root root   6263 Nov 14  2019 ksrsigner-20191114-190143.log
drwxr-xr-x 2 root root   8192 Nov 14  2019 \033[01;34mKSK39\033[0m
-rw-r--r-- 1 root root  52363 Nov 14  2019 ttyaudit-ttyS0-20191114-185111.log
-rw-r--r-- 1 root root  23869 Nov 14  2019 script-20191114.log
-rw-r--r-- 1 root root   6376 Oct 14  2021 ksrsigner-20211014-175632.log
drwxr-xr-x 2 root root   8192 Oct 14  2021 \033[01;34mKSK43\033[0m
-rw-r--r-- 1 root root   6391 Oct 14  2021 ksrsigner-20211014-190332.log
-rw-r--r-- 1 root root  64201 Oct 14  2021 ttyaudit-ttyS0-20211014-174505.log
-rw-r--r-- 1 root root  43058 Oct 14  2021 script-20211014.log
-rw-r--r-- 1 root root   6295 May 12  2022 ksrsigner-20220512-193033.log
drwxr-xr-x 2 root root   8192 May 12  2022 \033[01;34mKSK45\033[0m
-rw-r--r-- 1 root root 114456 May 12  2022 ttyaudit-ttyS0-20220512-181632.log
-rw-r--r-- 1 root root  25463 May 12  2022 script-20220512.log
-rw-r--r-- 1 root root   6265 Nov  3  2022 ksrsigner-20221103-181823.log
drwxr-xr-x 2 root root   8192 Nov  3  2022 \033[01;34mKSK47\033[0m
-rw-r--r-- 1 root root  15909 Nov  3  2022 ttyaudit-ttyS0-20221103-180106.log
-rw-r--r-- 1 root root  26616 Nov  3  2022 script-20221103.log
drwxr-xr-x 2 root root   8192 Apr 27  2023 \033[01;34mKSK49\033[0m
drwxr-xr-x 2 root root   8192 Apr 27  2023 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root   6274 Apr 27  2023 ksrsigner-20230427-181450.log
-rw-r--r-- 1 root root   1072 Apr 27  2023 kskm-keymaster-20230427-182232-931.log
-rw-r--r-- 1 root root   1965 Apr 27  2023 kskm-keymaster-20230427-182301-932.log
-rw-r--r-- 1 root root   2961 Apr 27  2023 KSKSlotDB.db
-rw-r--r-- 1 root root  46520 Apr 27  2023 ttyaudit-ttyS0-20230427-180005.log
-rw-r--r-- 1 root root  51776 Apr 27  2023 script-20230427.log
drwxr-xr-x 4 root root   8192 Nov 30 19:24 \033[01;34mKSK51\033[0m
-rw-r--r-- 1 root root  93387 Nov 30 20:48 ttyaudit-ttyUSB0-20231130-190131.log
-rw-r--r-- 1 root root  40960 Nov 30 20:51 script-20231130.log

./KSK29-0-C_to_D:
total 104
-rw-r--r-- 1 root root 20347 Apr 20  2017 skr.xml.20170427183853
-rw-r--r-- 1 root root 19556 Apr 20  2017 ksr-root-2017-q3-0-c_to_d.xml
-rw-r--r-- 1 root root   540 Apr 20  2017 kskschedule.json
-rw-r--r-- 1 root root 24419 Apr 27  2017 skr.xml
-rw-r--r-- 1 root root 24419 Apr 27  2017 skr-root-2017-q3-0-c_to_d.xml

./KSK29-1-D_to_C:
total 104
-rw-r--r-- 1 root root 20347 Apr 20  2017 skr.xml.20170427184519
-rw-r--r-- 1 root root 19556 Apr 20  2017 ksr-root-2017-q3-1-d_to_c.xml
-rw-r--r-- 1 root root   454 Apr 20  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr.xml
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr-root-2017-q3-1-d_to_c.xml

./KSK29-2-C_to_C:
total 104
-rw-r--r-- 1 root root 20347 Apr 20  2017 skr.xml.20170427184912
-rw-r--r-- 1 root root 19556 Apr 20  2017 ksr-root-2017-q3-2-c_to_c.xml
-rw-r--r-- 1 root root   454 Apr 20  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr.xml
-rw-r--r-- 1 root root 20347 Apr 27  2017 skr-root-2017-q3-2-c_to_c.xml

./KSK31-0-D_to_E:
```

```
total 128
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018181941
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-0-d_to_e.xml

./KSK31-1-E_to_D:
total 128
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018182803
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-1-e_to_d.xml

./KSK31-2-D_to_D:
total 128
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018183150
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-2-d_to_d.xml

./KSK31-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018183453
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 20347 Oct 18  2017 skr-root-2018-q1-3-c_to_c.xml

./KSK33-0-D_to_E:
total 128
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411183203
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr-root-2018-q3-0-d_to_e.xml

./KSK33-1-E_to_D:
total 128
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411183607
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr-root-2018-q3-1-e_to_d.xml

./KSK33-2-D_to_D:
total 128
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411183814
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 24928 Apr 11  2018 skr-root-2018-q3-2-d_to_d.xml

./KSK33-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Apr  4  2018 skr.xml.20180411184001
-rw-r--r-- 1 root root 19554 Apr  4  2018 ksr-root-2018-q3-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Apr  4  2018 kskschedule.json
-rw-r--r-- 1 root root 20347 Apr 11  2018 skr.xml
-rw-r--r-- 1 root root 20347 Apr 11  2018 skr-root-2018-q3-3-c_to_c.xml

./KSK35-0-E_to_F:
total 128
-rw-r--r-- 1 root root  1678 Oct 12  2018 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9  2018 ksr-root-2019-q1-0-e_to_f.xml
-rw-r--r-- 1 root root 24930 Nov  9  2018 skr.xml.20181115194236
-rw-r--r-- 1 root root 29640 Nov 15  2018 skr.xml
-rw-r--r-- 1 root root 29640 Nov 15  2018 skr-root-2019-q1-0-e_to_f.xml

./KSK35-1-F_to_G:
total 112
-rw-r--r-- 1 root root  1148 Oct 12  2018 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9  2018 ksr-root-2019-q1-1-f_to_g.xml
-rw-r--r-- 1 root root 24930 Nov  9  2018 skr.xml.20181115195208
-rw-r--r-- 1 root root 20367 Nov 15  2018 skr.xml
-rw-r--r-- 1 root root 20367 Nov 15  2018 skr-root-2019-q1-1-f_to_g.xml

./KSK35-2-E_to_E:
total 128
-rw-r--r-- 1 root root  1345 Oct 12  2018 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9  2018 ksr-root-2019-q1-2-e_to_e.xml
-rw-r--r-- 1 root root 24930 Nov  9  2018 skr.xml.20181115195448
-rw-r--r-- 1 root root 24948 Nov 15  2018 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15  2018 skr-root-2019-q1-2-e_to_e.xml

./KSK35-3-D_to_D:
total 128
-rw-r--r-- 1 root root  1344 Oct 12  2018 kskschedule.json
-rw-r--r-- 1 root root 19594 Nov  9  2018 ksr-root-2019-q1-3-d_to_d.xml
-rw-r--r-- 1 root root 24930 Nov  9  2018 skr.xml.20181115195652
-rw-r--r-- 1 root root 24948 Nov 15  2018 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15  2018 skr-root-2019-q1-3-d_to_d.xml

./KSK37:
total 104
-rw-r--r-- 1 root root 20369 May  8  2019 skr.xml.20190516190831
-rw-r--r-- 1 root root 19600 May  8  2019 ksr-root-2019-q3-0.xml
-rw-r--r-- 1 root root  1148 May  8  2019 kskschedule.json
-rw-r--r-- 1 root root 20369 May 16  2019 skr.xml
-rw-r--r-- 1 root root 20369 May 16  2019 skr-root-2019-q3-0.xml

./KSK39:
total 104
-rw-r--r-- 1 root root 20369 Nov  6  2019 skr.xml.20191114190143
-rw-r--r-- 1 root root 19600 Nov  6  2019 ksr-root-2020-q1-0.xml
-rw-r--r-- 1 root root  1148 Nov  6  2019 kskschedule.json
-rw-r--r-- 1 root root 20369 Nov 14  2019 skr.xml
-rw-r--r-- 1 root root 20369 Nov 14  2019 skr-root-2020-q1-0.xml

./KSK43:
total 104
-rw-r--r-- 1 root root 20369 Oct  2  2021 skr.xml.20211014175632
-rw-r--r-- 1 root root 19582 Oct  2  2021 ksr-root-2022-q1-0.xml
-rw-r--r-- 1 root root  1148 Oct  2  2021 kskschedule.json
-rw-r--r-- 1 root root 20369 Oct 14  2021 skr.xml
-rw-r--r-- 1 root root 20369 Oct 14  2021 skr-root-2022-q1-0.xml

./KSK45:
total 104
-rw-r--r-- 1 root root 20369 Apr 27  2022 skr.xml.20220512193033
-rw-r--r-- 1 root root 19600 Apr 27  2022 ksr-root-2022-q3-0.xml
-rw-r--r-- 1 root root  1148 Apr 27  2022 kskschedule.json
-rw-r--r-- 1 root root 20369 May 12  2022 skr.xml
-rw-r--r-- 1 root root 20369 May 12  2022 skr-root-2022-q3-0.xml

./KSK47:
```

```
total 104
-rw-r--r-- 1 root root 20369 Jul 11  2018 skr.xml.20221103181823
-rw-r--r-- 1 root root 19564 Jul 11  2018 ksr-root-2023-q1-0.xml
-rw-r--r-- 1 root root  1148 Jul 11  2018 kskschedule.json
-rw-r--r-- 1 root root 20369 Nov  3  2022 skr.xml
-rw-r--r-- 1 root root 20369 Nov  3  2022 skr-root-2023-q1-0.xml

./KSK49:
total 120
-rw-r--r-- 1 root root 20369 Apr 18  2023 skr.xml.20230427181450
-rw-r--r-- 1 root root 11189 Apr 18  2023 ksrsigner.yaml
-rw-r--r-- 1 root root 19600 Apr 18  2023 ksr-root-2023-q3-0.xml
-rw-r--r-- 1 root root  1148 Apr 18  2023 kskschedule.json
-rw-r--r-- 1 root root 20369 Apr 27  2023 skr.xml
-rw-r--r-- 1 root root 20369 Apr 27  2023 skr-root-2023-q3-0.xml

./tmp:
total 80
-rw-r--r-- 1 root root  880 May  2  2013 ksrsigner_20130502190252_5048_tmp_skr.xml
-rw-r--r-- 1 root root 1768 Apr 27  2023 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.3
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Apr 27  2023 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Apr 27  2023 skr.keybundle.0

./KSK51:
total 136
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11501 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 24832 Nov 30 19:24 skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11079 Nov 30 19:24 kskm-ksrsigner-20231130-192047-894.log
drwxr-xr-x 2 root root  8192 Nov 30 20:23 \033[01;34mHSM7E\033[0m
drwxr-xr-x 2 root root  8192 Nov 30 20:51 \033[01;34mHSM8E\033[0m

./KSK51/HSM7E:
total 176
-rw-r--r-- 1 root root   652 Nov 17 22:23 style.xsl
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11507 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 24832 Nov 30 20:19 HSM7E-skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11097 Nov 30 20:19 kskm-ksrsigner-20231130-201730-997.log
-rw-r--r-- 1 root root 22205 Nov 30 20:23 current
-rw-r--r-- 1 root root 22205 Nov 30 20:23 new

./KSK51/HSM8E:
total 176
-rw-r--r-- 1 root root   652 Nov 17 22:23 style.xsl
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11507 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11096 Nov 30 20:48 kskm-ksrsigner-20231130-204716-1058.log
-rw-r--r-- 1 root root 24832 Nov 30 20:48 HSM8E-skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 22205 Nov 30 20:51 current
-rw-r--r-- 1 root root 22205 Nov 30 20:51 new
\033[?2004h(kskm) root@coen:/media/HSMFD# diff -qr /media/HSMFD/K\007SK51/ /media/KSRFD/K
SK51/
\033[?2004h(kskm) root@coen:/media/HSMFD# umount /media/KSRFD/
\033[?2004h(kskm) root@coen:/media/HSMFD#
```

```
\033[?2004l

Script done on 2023-11-30 21:28:56+00:00 [COMMAND_EXIT_CODE="0"]
```

```
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0 H1903018 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0 H1903018 011403 ABL 030 : Tamper Challenge Response Key
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:40+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-11-30T19:02:40+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 ####################################
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 ####################################
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 ------------------------------------
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 vintoosTamperCount:     8
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 extampIMKTamperCount:   0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 tempdiffTamperCount:    0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 pfTamperCount:          8
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 restartTamperCount:     28
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 Current tamper bitmaps:
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 ----------------------
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T19:02:41+0000        ttyUSB0
2023-11-30T19:02:41+0000        ttyUSB0 ----------------------------------------
2023-11-30T19:02:41+0000        ttyUSB0
```

```
2023-11-30T19:02:41+0000 ttyUSB0
2023-11-30T19:02:41+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0 Board is P2020RDB
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0 board_smp_init: 2 cpu
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:42+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-11-30T19:02:42+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0 Starting next program at v0015183c
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0 Starting K-Series Kernel
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0 Sat Aug 17 03:22:19 1974
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:43+0000 ttyUSB0 Starting auditd v2.0 ... started.
2023-11-30T19:02:43+0000 ttyUSB0
2023-11-30T19:02:44+0000 ttyUSB0 Interface 0 configured for IPv6.
2023-11-30T19:02:44+0000 ttyUSB0
2023-11-30T19:02:44+0000 ttyUSB0 Interface 0 configured for IPv4.
2023-11-30T19:02:44+0000 ttyUSB0
2023-11-30T19:02:44+0000 ttyUSB0 Interface 1 configured for IPv6.
2023-11-30T19:02:44+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 Interface 1 configured for IPv4.
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 add net default: gateway ::: Network is unreachable
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 Starting USB driver...
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:45+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0 Running DES POST Test
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0 DES POST Test Passed
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0 Running Triple DES POST Test
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0 Triple DES POST Test Passed
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0 Running AES POST Test
2023-11-30T19:02:47+0000 ttyUSB0
2023-11-30T19:02:47+0000 ttyUSB0 AES POST Test Passed
2023-11-30T19:02:47+0000 ttyUSB0
```

```
2023-11-30T19:02:47+0000        ttyUSB0 Running SHA1 POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 SHA1 POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running SHA2 POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 SHA2 POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running RandomGen POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 RandomGen POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running RSA POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 RSA POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running DSA POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 DSA POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running SEED POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 SEED POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running ECC POST Test
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 ECC POST Test Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Running HMAC POST Tests
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 HMAC POST Tests Passed
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0 Audit on 17/8/1974 03:22:22 00100008
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:47+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Keyper 9860-2  Serial Number H1903018
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Memory Usage:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0    black store          596b
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0    statistics           112b
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0    other                116b
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
```

```
2023-11-30T19:02:48+0000        ttyUSB0 Network Configuration:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Interface 0:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0     IPv4: enabled
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0     IPv6: enabled
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C4:9D / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c49d/64
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Interface 1:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0     IPv4: enabled
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0     IPv6: enabled
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C4:9E / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c49e/64
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 HSM Port 0: 05000
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 HSM Port 1: 03000
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 Software Versions:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 CPLD Version:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 1.9
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:48+0000        ttyUSB0 SCR Firmware Version:
2023-11-30T19:02:48+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0 OROS-R2.99-R1.20
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0 HmcListener: Created IPv4 socket 12 on port 3000.
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0 HmcListener: Created IPv6 socket 13 on port 3000.
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:02:49+0000        ttyUSB0 Audit on 17/8/1974 03:22:24 00100003
2023-11-30T19:02:49+0000        ttyUSB0
2023-11-30T19:16:39+0000        ttyUSB0 Audit on 17/8/1974 03:36:14 00200069 478000018FED2972
2023-11-30T19:16:39+0000        ttyUSB0
2023-11-30T19:17:25+0000        ttyUSB0 Audit on 17/8/1974 03:37:00 00200069 47800000806D2972
2023-11-30T19:17:25+0000        ttyUSB0
2023-11-30T19:17:47+0000        ttyUSB0 Audit on 17/8/1974 03:37:22 00200069 4780000080AD2972
2023-11-30T19:17:47+0000        ttyUSB0
2023-11-30T19:17:50+0000        ttyUSB0
2023-11-30T19:17:50+0000        ttyUSB0
2023-11-30T19:17:50+0000        ttyUSB0 TcpListener: Created IPv4 socket 19 on port 5000.
2023-11-30T19:17:50+0000        ttyUSB0
```

```
2023-11-30T19:17:50+0000        ttyUSB0
2023-11-30T19:17:50+0000        ttyUSB0
2023-11-30T19:17:50+0000        ttyUSB0 TcpListener: Created IPv6 socket 20 on port 5000.
2023-11-30T19:17:50+0000        ttyUSB0
2023-11-30T19:17:50+0000        ttyUSB0 Audit on 17/8/1974 03:37:26 00100002
2023-11-30T19:17:50+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0 TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0 CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:20:47+0000        ttyUSB0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2023-11-30T19:20:47+0000        ttyUSB0
2023-11-30T19:24:02+0000        ttyUSB0
2023-11-30T19:24:02+0000        ttyUSB0
2023-11-30T19:24:02+0000        ttyUSB0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2023-11-30T19:24:02+0000        ttyUSB0
2023-11-30T19:28:29+0000        ttyUSB0 Audit on 17/8/1974 03:48:04 00200069 47800000826D2972
2023-11-30T19:28:29+0000        ttyUSB0
2023-11-30T19:28:52+0000        ttyUSB0 Audit on 17/8/1974 03:48:27 00200069 3980011621672A76
2023-11-30T19:28:52+0000        ttyUSB0
2023-11-30T19:29:14+0000        ttyUSB0 Audit on 17/8/1974 03:48:49 00200069 478000018FED2972
2023-11-30T19:29:14+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0 TcpListener: Closed IPv4 socket 19 on port 5000.
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0 TcpListener: Closed IPv6 socket 20 on port 5000.
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:29:18+0000        ttyUSB0 Audit on 17/8/1974 03:48:53 00100003
2023-11-30T19:29:18+0000        ttyUSB0
2023-11-30T19:33:25+0000        ttyUSB0 Audit on 17/8/1974 03:53:00 00200023 47800000081AD2972
2023-11-30T19:33:25+0000        ttyUSB0
2023-11-30T19:33:52+0000        ttyUSB0 Audit on 17/8/1974 03:53:27 00200023 3880000D4AA32A76
2023-11-30T19:33:52+0000        ttyUSB0
2023-11-30T19:34:24+0000        ttyUSB0 Audit on 17/8/1974 03:53:59 00200023 47800000081ED2972
2023-11-30T19:34:24+0000        ttyUSB0
2023-11-30T19:37:04+0000        ttyUSB0 Audit on 17/8/1974 03:56:39 0020002f 00400000F922156D
2023-11-30T19:37:04+0000        ttyUSB0
2023-11-30T19:37:59+0000        ttyUSB0 Audit on 17/8/1974 03:57:34 0020002f 00800002A48F156D
2023-11-30T19:37:59+0000        ttyUSB0
2023-11-30T19:38:56+0000        ttyUSB0 Audit on 17/8/1974 03:58:32 0020006f 0880004A83B3296D
2023-11-30T19:38:56+0000        ttyUSB0
2023-11-30T19:42:43+0000        ttyUSB0 Audit on 17/8/1974 04:02:19 00200023 3880000D58632A76
2023-11-30T19:42:43+0000        ttyUSB0
2023-11-30T19:43:11+0000        ttyUSB0 Audit on 17/8/1974 04:02:46 00200023 47800000816D2972
2023-11-30T19:43:11+0000        ttyUSB0
2023-11-30T19:43:45+0000        ttyUSB0 Audit on 17/8/1974 04:03:20 00200023 3880000D4AA32A76
2023-11-30T19:43:45+0000        ttyUSB0
2023-11-30T19:44:43+0000        ttyUSB0 Audit on 17/8/1974 04:04:18 0020002f 3980011654A72A76
2023-11-30T19:44:43+0000        ttyUSB0
2023-11-30T19:45:16+0000        ttyUSB0 Audit on 17/8/1974 04:04:51 0020002f 398001161F272A76
2023-11-30T19:45:16+0000        ttyUSB0
2023-11-30T19:45:28+0000        ttyUSB0 Audit on 17/8/1974 04:05:03 00200010 398001161F272A76
2023-11-30T19:45:28+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ÿ
2023-11-30T19:52:35+0000        ttyUSB0
```

```
2023-11-30T19:52:35+0000        ttyUSB0 H2110009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 H2110009 011403 ABL 030 : Tamper Challenge Response Key
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ###################################
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ###################################
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ------------------------------------
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 vintoosTamperCount:     3
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 extampIMKTamperCount:   0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 tempdiffTamperCount:    0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 pfTamperCount:          3
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 restartTamperCount:     8
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 Current tamper bitmaps:
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ----------------------
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0 ----------------------------------------
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
2023-11-30T19:52:35+0000        ttyUSB0
```

```
2023-11-30T19:52:36+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:36+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:36+0000 ttyUSB0 Board is P2020RDB
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:36+0000 ttyUSB0 board_smp_init: 2 cpu
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:36+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-11-30T19:52:36+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 Starting next program at v0015183c
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 Starting K-Series Kernel
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 Sat Jun 20 06:29:42 1970
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 Starting auditd v2.0 ... started.
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:38+0000 ttyUSB0 Interface 0 configured for IPv6.
2023-11-30T19:52:38+0000 ttyUSB0
2023-11-30T19:52:39+0000 ttyUSB0 Interface 0 configured for IPv4.
2023-11-30T19:52:39+0000 ttyUSB0
2023-11-30T19:52:39+0000 ttyUSB0 Interface 1 configured for IPv6.
2023-11-30T19:52:39+0000 ttyUSB0
2023-11-30T19:52:39+0000 ttyUSB0 Interface 1 configured for IPv4.
2023-11-30T19:52:39+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0 add net default: gateway ::: Network is unreachable
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0 Starting USB driver...
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:40+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 Running DES POST Test
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 DES POST Test Passed
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 Running Triple DES POST Test
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 Triple DES POST Test Passed
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 Running AES POST Test
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 AES POST Test Passed
2023-11-30T19:52:41+0000 ttyUSB0
2023-11-30T19:52:41+0000 ttyUSB0 Running SHA1 POST Test
2023-11-30T19:52:41+0000 ttyUSB0
```

```
2023-11-30T19:52:41+0000        ttyUSB0 SHA1 POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 Running SHA2 POST Test
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 SHA2 POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 Running RandomGen POST Test
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 RandomGen POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 Running RSA POST Test
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 RSA POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 Running DSA POST Test
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 DSA POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 Running SEED POST Test
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 SEED POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:41+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0 Running ECC POST Test
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0 ECC POST Test Passed
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0 Running HMAC POST Tests
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0 HMAC POST Tests Passed
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0 Audit on 20/6/1970 06:29:45 00100008
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:42+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Keyper 9860-2  Serial Number H2110009
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Memory Usage:
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0    black store          44b
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0    statistics           112b
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0    other                116b
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Network Configuration:
2023-11-30T19:52:43+0000        ttyUSB0
```

```
2023-11-30T19:52:43+0000        ttyUSB0 Interface 0:
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0     IPv4: enabled
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0     IPv6: enabled
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:4E / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c94e/64
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Interface 1:
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0     IPv4: enabled
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0     IPv6: enabled
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:4F / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c94f/64
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 HSM Port 0: 05000
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 HSM Port 1: 03000
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Software Versions:
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 CPLD Version:
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 1.9
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 SCR Firmware Version:
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 OROS-R2.99-R1.20
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:52:43+0000        ttyUSB0 Audit on 20/6/1970 06:29:47 00100001
2023-11-30T19:52:43+0000        ttyUSB0
2023-11-30T19:53:57+0000        ttyUSB0 Audit on 20/6/1970 06:31:01 00200035 3980011654A72A76
2023-11-30T19:53:57+0000        ttyUSB0
2023-11-30T19:54:14+0000        ttyUSB0 Audit on 20/6/1970 06:31:17 00200035 398001161F272A76
2023-11-30T19:54:14+0000        ttyUSB0
2023-11-30T19:54:14+0000        ttyUSB0 Audit on 20/6/1970 06:31:18 0020000e 398001161F272A76
2023-11-30T19:54:14+0000        ttyUSB0
2023-11-30T19:55:31+0000        ttyUSB0 Audit on 20/6/1970 06:32:35 00200023 47800000816D2972
2023-11-30T19:55:31+0000        ttyUSB0
2023-11-30T19:55:55+0000        ttyUSB0 Audit on 20/6/1970 06:32:58 00200023 4780000081AD2972
2023-11-30T19:55:55+0000        ttyUSB0
2023-11-30T19:56:19+0000        ttyUSB0 Audit on 20/6/1970 06:33:22 00200023 3880000D58632A76
2023-11-30T19:56:19+0000        ttyUSB0
2023-11-30T19:56:31+0000        ttyUSB0 Audit on 20/6/1970 06:33:34 00200056
2023-11-30T19:56:31+0000        ttyUSB0
2023-11-30T19:57:00+0000        ttyUSB0 Audit on 20/6/1970 06:34:04 00200081
2023-11-30T19:57:00+0000        ttyUSB0
2023-11-30T19:57:09+0000        ttyUSB0 Audit on 20/6/1970 06:34:13 00200054
2023-11-30T19:57:09+0000        ttyUSB0
2023-11-30T19:57:11+0000        ttyUSB0 Audit on 20/6/1970 06:34:15 00200028
2023-11-30T19:57:11+0000        ttyUSB0
```

```
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:14+0000        ttyUSB0 HmcListener: Created IPv4 socket 9 on port 3000.
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:14+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:14+0000        ttyUSB0 Audit on 20/6/1970 06:34:18 00100003
2023-11-30T19:57:14+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 Audit on 20/6/1970 06:34:18 00100005
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 Shutting down daemons...
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 AuditBuffer rx'd [-1] (3)
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 shutting down audit service.
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 Terminated
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 HmcListener::accept(): No such process
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:15+0000        ttyUSB0 Shutting down filesystems...
2023-11-30T19:57:15+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 H2110009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 H2110009 011403 ABL 030 : Tamper Challenge Response Key
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 ###################################
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 ###################################
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 ------------------------------------
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 vintoosTamperCount:     3
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T19:57:17+0000        ttyUSB0
2023-11-30T19:57:17+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T19:57:17+0000        ttyUSB0
```

```
2023-11-30T19:57:17+0000 ttyUSB0 extampIMKTamperCount:   0
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:17+0000 ttyUSB0 tempdiffTamperCount:    0
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:17+0000 ttyUSB0 pfTamperCount:          3
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:17+0000 ttyUSB0 restartTamperCount:     8
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:17+0000 ttyUSB0 Current tamper bitmaps:
2023-11-30T19:57:17+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0 ========================
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0 ========================================
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:18+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0 Jumping to startup @ 0x001037B4
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0 Board is P2020RDB
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0 board_smp_init: 2 cpu
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:19+0000 ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-11-30T19:57:19+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0 Starting next program at v0015183c
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0 Starting K-Series Kernel
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0 Sat Jun 20 06:34:25 1970
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:20+0000 ttyUSB0 Starting auditd v2.0 ... started.
2023-11-30T19:57:20+0000 ttyUSB0
2023-11-30T19:57:21+0000 ttyUSB0 Interface 0 configured for IPv6.
2023-11-30T19:57:21+0000 ttyUSB0
2023-11-30T19:57:21+0000 ttyUSB0 Interface 0 configured for IPv4.
2023-11-30T19:57:21+0000 ttyUSB0
2023-11-30T19:57:21+0000 ttyUSB0 Interface 1 configured for IPv6.
2023-11-30T19:57:21+0000 ttyUSB0
2023-11-30T19:57:22+0000 ttyUSB0 Interface 1 configured for IPv4.
2023-11-30T19:57:22+0000 ttyUSB0
2023-11-30T19:57:22+0000 ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T19:57:22+0000 ttyUSB0
2023-11-30T19:57:22+0000 ttyUSB0 add net default: gateway ::: Network is unreachable
2023-11-30T19:57:22+0000 ttyUSB0
```

```
2023-11-30T19:57:22+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T19:57:22+0000        ttyUSB0
2023-11-30T19:57:22+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-11-30T19:57:22+0000        ttyUSB0
2023-11-30T19:57:22+0000        ttyUSB0 Starting USB driver...
2023-11-30T19:57:22+0000        ttyUSB0
2023-11-30T19:57:22+0000        ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-11-30T19:57:22+0000        ttyUSB0
2023-11-30T19:57:22+0000        ttyUSB0
2023-11-30T19:57:22+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running DES POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 DES POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running Triple DES POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Triple DES POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running AES POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 AES POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running SHA1 POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 SHA1 POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running SHA2 POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 SHA2 POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running RandomGen POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 RandomGen POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running RSA POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 RSA POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running DSA POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 DSA POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running SEED POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 SEED POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running ECC POST Test
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 ECC POST Test Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 Running HMAC POST Tests
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0 HMAC POST Tests Passed
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
```

```
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:24+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Keyper 9860-2  Serial Number H2110009
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Memory Usage:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0    black store          272b
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0    statistics           112b
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0    other                116b
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Network Configuration:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Interface 0:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0     IPv4: enabled
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0     IPv6: enabled
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:4E / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c94e/64
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Interface 1:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0     IPv4: enabled
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0     IPv6: enabled
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:4F / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c94f/64
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 HSM Port 0: 05000
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 HSM Port 1: 03000
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Software Versions:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 CPLD Version:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 1.9
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 SCR Firmware Version:
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 OROS-R2.99-R1.20
2023-11-30T19:57:25+0000        ttyUSB0
```

```
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 HmcListener: Created IPv4 socket 9 on port 3000.
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 HmcListener: Created IPv6 socket 10 on port 3000.
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:57:25+0000        ttyUSB0 Audit on 20/6/1970 06:34:29 00100003
2023-11-30T19:57:25+0000        ttyUSB0
2023-11-30T19:58:39+0000        ttyUSB0 Audit on 20/6/1970 06:35:44 0020006c
2023-11-30T19:58:39+0000        ttyUSB0
2023-11-30T19:59:08+0000        ttyUSB0 Audit on 20/6/1970 06:36:12 0020006b 3880000C2D232A76
2023-11-30T19:59:08+0000        ttyUSB0
2023-11-30T19:59:32+0000        ttyUSB0 Audit on 20/6/1970 06:36:37 0020006b 3880000C2E232A76
2023-11-30T19:59:32+0000        ttyUSB0
2023-11-30T19:59:55+0000        ttyUSB0 Audit on 20/6/1970 06:36:59 0020006b 3880000C41232A76
2023-11-30T19:59:55+0000        ttyUSB0
2023-11-30T20:00:21+0000        ttyUSB0 Audit on 20/6/1970 06:37:25 00200039
2023-11-30T20:00:21+0000        ttyUSB0
2023-11-30T20:00:30+0000        ttyUSB0 Audit on 20/6/1970 06:37:34 0020003b
2023-11-30T20:00:30+0000        ttyUSB0
2023-11-30T20:00:40+0000        ttyUSB0 Audit on 20/6/1970 06:37:45 00200041
2023-11-30T20:00:40+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 HSM Status
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 ==================
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Keyper 9860-2
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Serial Number H2110009
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Date(dd/mm/yyyy) 20/6/1970  Time 6:38:40
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Software Versions:
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 CPLD Version:
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 1.9
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 SCR Firmware Version:
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 OROS-R2.99-R1.20
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
```

```
2023-11-30T20:01:36+0000	ttyUSB0 Memory Usage:
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 RAM (free/total)	192Mb/256Mb
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 Flash (free/total)	127Mb/128Mb
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    black store	452b
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    statistics	112b
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    other	116b
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 RedStore (free/total)	107Kb/128Kb
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 Network Configuration:
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 Interface 0:
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    IPv4: enabled
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    IPv6: enabled
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    MAC/IP address(es): 00:E0:6C:00:C9:4E / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c94e/64
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        capabilities tx=0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        enabled=0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        address: 00:e0:6c:00:c9:4e
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        media: Ethernet none
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        inet6 2001::2e0:6cff:fe00:c94e prefixlen 64
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        inet6 fe80::2e0:6cff:fe00:c94e%tsec0 prefixlen 64 scopeid 0x2
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 Interface 1:
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    IPv4: enabled
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    IPv6: enabled
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0    MAC/IP address(es): 00:E0:6C:00:C9:4F / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c94f/64
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0 tsec1: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        capabilities tx=0
2023-11-30T20:01:36+0000	ttyUSB0
2023-11-30T20:01:36+0000	ttyUSB0        enabled=0
2023-11-30T20:01:36+0000	ttyUSB0
```

```
2023-11-30T20:01:36+0000        ttyUSB0         address: 00:e0:6c:00:c9:4f
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0         media: Ethernet none
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0         inet 192.168.1.2 netmask 0xffffff00 broadcast 192.168.1.255
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0         inet6 2001::1:2e0:6cff:fe00:c94f prefixlen 64
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0         inet6 fe80::2e0:6cff:fe00:c94f%tsec1 prefixlen 64 scopeid 0x3
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 HSM Port 0: 05000
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 HSM Port 1: 03000
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Current HSM State: Secured Off-line
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Modes: (1=Enabled 0=Disabled)
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Global Key Export    1  App Key Import       0  App Key Export       0  Asymmetric Key Gen   1
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 Symmetric Key Gen    1  Symmetric Key Derive 0  Signing              1  Signature Verify     1
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:36+0000        ttyUSB0 MAC Generation       1  MAC Verification     1  Encrypt / Decrypt    1  Delete Asym Key      1
2023-11-30T20:01:36+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Delete Sym Key       1  Output Key Details   1  Output Key Summary   1  Suite B Algorithms   1
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Non Suite B Algs     1  Auto Online          0  Remote Management    0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Other Modes:
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 AES SMK                 Set Offline             FIPS Mode
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Battery ok
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 ###################################
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 ###################################
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 ------------------------------------
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 vintoosTamperCount:     0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T20:01:37+0000        ttyUSB0
```

```
2023-11-30T20:01:37+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 extampIMKTamperCount:   0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 tempdiffTamperCount:    0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 pfTamperCount:          0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 restartTamperCount:     0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Current tamper bitmaps:
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 ======================
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 lastTamper bitmap:      0x0000 0b .... .... .... ....
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 ========================================
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 \000============================================
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 DRBG Instantiate Health Test On Demand Passed
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 DRBG Generate Health Test On Demand Passed
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:01:37+0000        ttyUSB0 DRBG Reseed Health Test On Demand Passed
2023-11-30T20:01:37+0000        ttyUSB0
2023-11-30T20:09:08+0000        ttyUSB0 Audit on 20/6/1970 06:46:13 0020006b 3880000C2D632A76
2023-11-30T20:09:08+0000        ttyUSB0
2023-11-30T20:09:41+0000        ttyUSB0 Audit on 20/6/1970 06:46:46 0020006b 3880000B42632A76
2023-11-30T20:09:41+0000        ttyUSB0
2023-11-30T20:10:05+0000        ttyUSB0 Audit on 20/6/1970 06:47:10 0020006b 3880000C2D232A76
2023-11-30T20:10:05+0000        ttyUSB0
2023-11-30T20:11:11+0000        ttyUSB0 Audit on 20/6/1970 06:48:15 00200025 3880000DD8E32A76
2023-11-30T20:11:11+0000        ttyUSB0
2023-11-30T20:11:29+0000        ttyUSB0 Audit on 20/6/1970 06:48:33 00200025 3980011675A72A76
2023-11-30T20:11:29+0000        ttyUSB0
2023-11-30T20:11:49+0000        ttyUSB0 Audit on 20/6/1970 06:48:53 00200025 3980011675E72A76
2023-11-30T20:11:49+0000        ttyUSB0
2023-11-30T20:11:51+0000        ttyUSB0 Audit on 20/6/1970 06:48:55 00200005
2023-11-30T20:11:51+0000        ttyUSB0
2023-11-30T20:13:25+0000        ttyUSB0 Audit on 20/6/1970 06:50:29 00200016 Klajeyz
2023-11-30T20:13:25+0000        ttyUSB0
2023-11-30T20:13:25+0000        ttyUSB0 Audit on 20/6/1970 06:50:29 00200015 4780000180AD2972
2023-11-30T20:13:25+0000        ttyUSB0
2023-11-30T20:13:25+0000        ttyUSB0 Audit on 20/6/1970 06:50:30 00200018
2023-11-30T20:13:25+0000        ttyUSB0
```

```
2023-11-30T20:14:13+0000        ttyUSB0 Audit on 20/6/1970 06:51:18 00200016 Kmrfl3b
2023-11-30T20:14:13+0000        ttyUSB0
2023-11-30T20:14:13+0000        ttyUSB0 Audit on 20/6/1970 06:51:18 00200015 3F400031F8CA2A77
2023-11-30T20:14:13+0000        ttyUSB0
2023-11-30T20:14:14+0000        ttyUSB0 Audit on 20/6/1970 06:51:18 00200018
2023-11-30T20:14:14+0000        ttyUSB0
2023-11-30T20:15:22+0000        ttyUSB0 Audit on 20/6/1970 06:52:26 00200069 3980011621672A76
2023-11-30T20:15:22+0000        ttyUSB0
2023-11-30T20:15:43+0000        ttyUSB0 Audit on 20/6/1970 06:52:48 00200069 478000000806D2972
2023-11-30T20:15:43+0000        ttyUSB0
2023-11-30T20:16:07+0000        ttyUSB0 Audit on 20/6/1970 06:53:11 00200069 478000000826D2972
2023-11-30T20:16:07+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0 TcpListener: Created IPv4 socket 20 on port 5000.
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0 TcpListener: Created IPv6 socket 21 on port 5000.
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:16:09+0000        ttyUSB0 Audit on 20/6/1970 06:53:13 00100002
2023-11-30T20:16:09+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0 TcpListener: Accepted connection on socket 22 from address 192.168.0.1.
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0 CryptoTask: Closing connection on socket 22 from address 192.168.0.1.
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:17:30+0000        ttyUSB0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2023-11-30T20:17:30+0000        ttyUSB0
2023-11-30T20:19:42+0000        ttyUSB0
2023-11-30T20:19:42+0000        ttyUSB0
2023-11-30T20:19:42+0000        ttyUSB0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2023-11-30T20:19:42+0000        ttyUSB0
2023-11-30T20:24:53+0000        ttyUSB0 Audit on 20/6/1970 07:01:57 00200069 478000000806D2972
2023-11-30T20:24:53+0000        ttyUSB0
2023-11-30T20:25:15+0000        ttyUSB0 Audit on 20/6/1970 07:02:19 00200069 478000018FED2972
2023-11-30T20:25:15+0000        ttyUSB0
2023-11-30T20:25:35+0000        ttyUSB0 Audit on 20/6/1970 07:02:39 00200069 478000000826D2972
2023-11-30T20:25:35+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0 TcpListener: Closed IPv4 socket 20 on port 5000.
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0 TcpListener: Closed IPv6 socket 21 on port 5000.
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:25:41+0000        ttyUSB0 Audit on 20/6/1970 07:02:45 00100003
2023-11-30T20:25:41+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 H2110010 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
```

```
2023-11-30T20:31:06+0000        ttyUSB0 H2110010 011403 ABL 030 : Tamper Challenge Response Key
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ###################################
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ###################################
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ------------------------------------
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 vintoosTamperCount:     3
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 extampIMKTamperCount:   0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 tempdiffTamperCount:    0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 pfTamperCount:          3
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 restartTamperCount:     8
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 Current tamper bitmaps:
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ----------------------
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0 ----------------------------------------
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:06+0000        ttyUSB0
2023-11-30T20:31:08+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-11-30T20:31:08+0000        ttyUSB0
2023-11-30T20:31:08+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2023-11-30T20:31:08+0000        ttyUSB0
2023-11-30T20:31:08+0000        ttyUSB0 Board is P2020RDB
2023-11-30T20:31:08+0000        ttyUSB0
2023-11-30T20:31:08+0000        ttyUSB0 board_smp_init: 2 cpu
2023-11-30T20:31:08+0000        ttyUSB0
```

```
2023-11-30T20:31:08+0000        ttyUSB0
2023-11-30T20:31:08+0000        ttyUSB0
2023-11-30T20:31:08+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-11-30T20:31:08+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0 Starting next program at v0015183c
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0 Starting K-Series Kernel
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0 Sat Jun 20 07:25:58 1970
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:09+0000        ttyUSB0 Starting auditd v2.0 ... started.
2023-11-30T20:31:09+0000        ttyUSB0
2023-11-30T20:31:10+0000        ttyUSB0 Interface 0 configured for IPv6.
2023-11-30T20:31:10+0000        ttyUSB0
2023-11-30T20:31:10+0000        ttyUSB0 Interface 0 configured for IPv4.
2023-11-30T20:31:10+0000        ttyUSB0
2023-11-30T20:31:10+0000        ttyUSB0 Interface 1 configured for IPv6.
2023-11-30T20:31:10+0000        ttyUSB0
2023-11-30T20:31:10+0000        ttyUSB0 Interface 1 configured for IPv4.
2023-11-30T20:31:10+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0 Starting USB driver...
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:11+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running DES POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 DES POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running Triple DES POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Triple DES POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running AES POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 AES POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running SHA1 POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 SHA1 POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running SHA2 POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 SHA2 POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running RandomGen POST Test
2023-11-30T20:31:13+0000        ttyUSB0
```

```
2023-11-30T20:31:13+0000        ttyUSB0 RandomGen POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running RSA POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 RSA POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running DSA POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 DSA POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running SEED POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 SEED POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running ECC POST Test
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 ECC POST Test Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 Running HMAC POST Tests
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:13+0000        ttyUSB0 HMAC POST Tests Passed
2023-11-30T20:31:13+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Audit on 20/6/1970 07:26:01 00100008
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Keyper 9860-2  Serial Number H2110010
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Memory Usage:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0    black store          44b
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0    statistics           112b
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0    other                116b
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Network Configuration:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Interface 0:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0     IPv4: enabled
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0     IPv6: enabled
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:51 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c951/64
2023-11-30T20:31:14+0000        ttyUSB0
```

```
2023-11-30T20:31:14+0000        ttyUSB0 Interface 1:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0     IPv4: enabled
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0     IPv6: enabled
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:52 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c952/64
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 HSM Port 0: 05000
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 HSM Port 1: 03000
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 Software Versions:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 CPLD Version:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 1.9
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 SCR Firmware Version:
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0 OROS-R2.99-R1.20
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:14+0000        ttyUSB0
2023-11-30T20:31:15+0000        ttyUSB0 Audit on 20/6/1970 07:26:03 00100001
2023-11-30T20:31:15+0000        ttyUSB0
2023-11-30T20:32:11+0000        ttyUSB0 Audit on 20/6/1970 07:26:59 00200035 398001161F272A76
2023-11-30T20:32:11+0000        ttyUSB0
2023-11-30T20:32:26+0000        ttyUSB0 Audit on 20/6/1970 07:27:14 00200035 3980011654A72A76
2023-11-30T20:32:26+0000        ttyUSB0
2023-11-30T20:32:26+0000        ttyUSB0 Audit on 20/6/1970 07:27:15 0020000e 3980011654A72A76
2023-11-30T20:32:26+0000        ttyUSB0
2023-11-30T20:33:23+0000        ttyUSB0 Audit on 20/6/1970 07:28:11 00200023 4780000081AD2972
2023-11-30T20:33:23+0000        ttyUSB0
2023-11-30T20:33:44+0000        ttyUSB0 Audit on 20/6/1970 07:28:32 00200023 3880000D4AA32A76
2023-11-30T20:33:44+0000        ttyUSB0
2023-11-30T20:34:05+0000        ttyUSB0 Audit on 20/6/1970 07:28:53 00200023 4780000081ED2972
2023-11-30T20:34:05+0000        ttyUSB0
2023-11-30T20:34:17+0000        ttyUSB0 Audit on 20/6/1970 07:29:05 00200056
2023-11-30T20:34:17+0000        ttyUSB0
2023-11-30T20:35:05+0000        ttyUSB0 Audit on 20/6/1970 07:29:53 00200081
2023-11-30T20:35:05+0000        ttyUSB0
2023-11-30T20:35:13+0000        ttyUSB0 Audit on 20/6/1970 07:30:01 00200054
2023-11-30T20:35:13+0000        ttyUSB0
2023-11-30T20:35:15+0000        ttyUSB0 Audit on 20/6/1970 07:30:03 00200028
2023-11-30T20:35:15+0000        ttyUSB0
2023-11-30T20:35:17+0000        ttyUSB0
2023-11-30T20:35:17+0000        ttyUSB0
2023-11-30T20:35:17+0000        ttyUSB0 HmcListener: Created IPv4 socket 9 on port 3000.
2023-11-30T20:35:17+0000        ttyUSB0
2023-11-30T20:35:17+0000        ttyUSB0
2023-11-30T20:35:17+0000        ttyUSB0
2023-11-30T20:35:17+0000        ttyUSB0 HmcListener: Created IPv6 socket 11 on port 3000.
2023-11-30T20:35:17+0000        ttyUSB0
```

```
2023-11-30T20:35:17+0000        ttyUSB0 Audit on 20/6/1970 07:30:06 00100003
2023-11-30T20:35:17+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 Audit on 20/6/1970 07:30:06 00100005
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 Shutting down daemons...
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 AuditBuffer rx'd [-1] (3)
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 shutting down audit service.
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 Terminated
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 HmcListener::accept(): No such process
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:18+0000        ttyUSB0 Shutting down filesystems...
2023-11-30T20:35:18+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 H2110010 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 BBL CRC32: 0xDBC9B9F2
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 Running applicationBootLoader at 0xEFDC0000
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 H2110010 011403 ABL 030 : Tamper Challenge Response Key
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ABL CRC32: 0xE7E0FA6A
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ###################################
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ###################################
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ===================================
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 vintoosTamperCount:     3
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 extampIMKTamperCount:   0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 tempdiffTamperCount:    0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 pfTamperCount:          3
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 restartTamperCount:     8
2023-11-30T20:35:20+0000        ttyUSB0
```

```
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 Current tamper bitmaps:
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ----------------------
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0 ----------------------------------------
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:20+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0 Running cryptoApplication at 0xEBF00000
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0 Jumping to startup @ 0x001037B4
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0 Board is P2020RDB
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0 board_smp_init: 2 cpu
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:22+0000        ttyUSB0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-11-30T20:35:22+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0 Starting next program at v0015183c
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0 Starting K-Series Kernel
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0 Sat Jun 20 07:30:12 1970
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:23+0000        ttyUSB0 Starting auditd v2.0 ... started.
2023-11-30T20:35:23+0000        ttyUSB0
2023-11-30T20:35:24+0000        ttyUSB0 Interface 0 configured for IPv6.
2023-11-30T20:35:24+0000        ttyUSB0
2023-11-30T20:35:24+0000        ttyUSB0 Interface 0 configured for IPv4.
2023-11-30T20:35:24+0000        ttyUSB0
2023-11-30T20:35:24+0000        ttyUSB0 Interface 1 configured for IPv6.
2023-11-30T20:35:24+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 Interface 1 configured for IPv4.
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 add net default: gateway ::: Network is unreachable
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 route: writing to routing socket: Network is unreachable
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 add net default: gateway 0.0.0.0: Network is unreachable
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 Starting USB driver...
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-11-30T20:35:25+0000        ttyUSB0
```

```
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:25+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running DES POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 DES POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running Triple DES POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Triple DES POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running AES POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 AES POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running SHA1 POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 SHA1 POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running SHA2 POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 SHA2 POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running RandomGen POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 RandomGen POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running RSA POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 RSA POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running DSA POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 DSA POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running SEED POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 SEED POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running RIPEMD160 POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 RIPEMD160 POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running ECC POST Test
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 ECC POST Test Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 Running HMAC POST Tests
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0 HMAC POST Tests Passed
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:27+0000        ttyUSB0
2023-11-30T20:35:28+0000        ttyUSB0 Keyper 9860-2  Serial Number H2110010
2023-11-30T20:35:28+0000        ttyUSB0
2023-11-30T20:35:28+0000        ttyUSB0
2023-11-30T20:35:28+0000        ttyUSB0
2023-11-30T20:35:28+0000        ttyUSB0 Memory Usage:
2023-11-30T20:35:28+0000        ttyUSB0
```

```
2023-11-30T20:35:28+0000 ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0    black store          272b
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0    statistics           112b
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0    other                116b
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 Network Configuration:
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 Interface 0:
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0     IPv4: enabled
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0     IPv6: enabled
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:51 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c951/64
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 Interface 1:
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0     IPv4: enabled
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0     IPv6: enabled
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:52 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c952/64
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 HSM Port 0: 05000
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 HSM Port 1: 03000
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 Software Versions:
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 CPLD Version:
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 1.9
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 SCR Firmware Version:
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 OROS-R2.99-R1.20
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0 HmcListener: Created IPv4 socket 9 on port 3000.
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
2023-11-30T20:35:28+0000 ttyUSB0
```

```
2023-11-30T20:35:28+0000        ttyUSB0 HmcListener: Created IPv6 socket 10 on port 3000.
2023-11-30T20:35:28+0000        ttyUSB0
2023-11-30T20:35:28+0000        ttyUSB0 Audit on 20/6/1970 07:30:16 00100003
2023-11-30T20:35:28+0000        ttyUSB0
2023-11-30T20:36:01+0000        ttyUSB0 Audit on 20/6/1970 07:30:49 0020006b 3880000C2D232A76
2023-11-30T20:36:01+0000        ttyUSB0
2023-11-30T20:36:21+0000        ttyUSB0 Audit on 20/6/1970 07:31:09 0020006b 3880000C2E232A76
2023-11-30T20:36:21+0000        ttyUSB0
2023-11-30T20:36:42+0000        ttyUSB0 Audit on 20/6/1970 07:31:31 0020006b 3880000C41232A76
2023-11-30T20:36:42+0000        ttyUSB0
2023-11-30T20:37:01+0000        ttyUSB0 Audit on 20/6/1970 07:31:49 00200039
2023-11-30T20:37:01+0000        ttyUSB0
2023-11-30T20:37:06+0000        ttyUSB0 Audit on 20/6/1970 07:31:55 0020003b
2023-11-30T20:37:06+0000        ttyUSB0
2023-11-30T20:37:13+0000        ttyUSB0 Audit on 20/6/1970 07:32:01 00200041
2023-11-30T20:37:13+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 HSM Status
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 ------------------
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 Keyper 9860-2
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 Serial Number H2110010
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 Date(dd/mm/yyyy) 20/6/1970  Time 7:32:28
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 Software Versions:
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 BBL 030 ABL 021 App 034
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 CPLD Version:
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 1.9
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 SCR Firmware Version:
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 OROS-R2.99-R1.20
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 Memory Usage:
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 RAM (free/total)        192Mb/256Mb
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0 Flash (free/total)      127Mb/128Mb
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0    black store          452b
2023-11-30T20:37:39+0000        ttyUSB0
2023-11-30T20:37:39+0000        ttyUSB0    statistics           112b
2023-11-30T20:37:39+0000        ttyUSB0
```

```
2023-11-30T20:37:39+0000 ttyUSB0    other                116b
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0 RedStore (free/total)   107Kb/128Kb
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0 Network Configuration:
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0 Interface 0:
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0     IPv4: enabled
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:39+0000 ttyUSB0     IPv6: enabled
2023-11-30T20:37:39+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:51 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c951/64
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0 tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         capabilities tx=0
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         enabled=0
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         address: 00:e0:6c:00:c9:51
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         media: Ethernet none
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         inet6 2001::2e0:6cff:fe00:c951 prefixlen 64
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         inet6 fe80::2e0:6cff:fe00:c951%tsec0 prefixlen 64 scopeid 0x2
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0 Interface 1:
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0     IPv4: enabled
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0     IPv6: enabled
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C9:52 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c952/64
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0 tsec1: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         capabilities tx=0
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         enabled=0
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         address: 00:e0:6c:00:c9:52
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         media: Ethernet none
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         inet 192.168.1.2 netmask 0xffffff00 broadcast 192.168.1.255
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         inet6 2001::1:2e0:6cff:fe00:c952 prefixlen 64
2023-11-30T20:37:40+0000 ttyUSB0
2023-11-30T20:37:40+0000 ttyUSB0         inet6 fe80::2e0:6cff:fe00:c952%tsec1 prefixlen 64 scopeid 0x3
2023-11-30T20:37:40+0000 ttyUSB0
```

```
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 HSM Port 0: 05000
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 HSM Port 1: 03000
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Current HSM State: Secured Off-line
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Modes: (1=Enabled 0=Disabled)
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Global Key Export    1  App Key Import       0  App Key Export       0  Asymmetric Key Gen   1
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Symmetric Key Gen    1  Symmetric Key Derive 0  Signing              1  Signature Verify     1
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 MAC Generation       1  MAC Verification     1  Encrypt / Decrypt    1  Delete Asym Key      1
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Delete Sym Key       1  Output Key Details   1  Output Key Summary   1  Suite B Algorithms   1
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Non Suite B Algs     1  Auto Online          0  Remote Management    0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Other Modes:
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 AES SMK                 Set Offline             FIPS Mode
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Battery ok
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 ###################################
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 ###     ABL tamper records       ###
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 ###################################
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Current Tamper Counts (decimal 0-255):
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 ===================================
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 vextoosTamperCount:     0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 vintoosTamperCount:     0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 vbboosTamperCount:      0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 maxstrtempTamperCount:  0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 minstrtempTamperCount:  0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 meshTamperCount:        0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 extampSMKTamperCount:   0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 extampIMKTamperCount:   0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 tempdiffTamperCount:    0
2023-11-30T20:37:40+0000        ttyUSB0
```

```
2023-11-30T20:37:40+0000        ttyUSB0 pfTamperCount:          0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 restartTamperCount:     0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Current tamper bitmaps:
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 ======================
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 lastTamper bitmap:      0x0000 0b .... .... .... ....
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 Bitmapped Change Record (most recent first):
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 ========================================
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 \000========================================
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 DRBG Instantiate Health Test On Demand Passed
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 DRBG Generate Health Test On Demand Passed
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:37:40+0000        ttyUSB0 DRBG Reseed Health Test On Demand Passed
2023-11-30T20:37:40+0000        ttyUSB0
2023-11-30T20:39:12+0000        ttyUSB0 Audit on 20/6/1970 07:34:00 0020006b 3880000C41232A76
2023-11-30T20:39:12+0000        ttyUSB0
2023-11-30T20:39:40+0000        ttyUSB0 Audit on 20/6/1970 07:34:28 0020006b 3880000C2D632A76
2023-11-30T20:39:40+0000        ttyUSB0
2023-11-30T20:40:00+0000        ttyUSB0 Audit on 20/6/1970 07:34:48 0020006b 3880000C2E232A76
2023-11-30T20:40:00+0000        ttyUSB0
2023-11-30T20:41:03+0000        ttyUSB0 Audit on 20/6/1970 07:35:51 00200025 3980011649A72A76
2023-11-30T20:41:03+0000        ttyUSB0
2023-11-30T20:41:18+0000        ttyUSB0 Audit on 20/6/1970 07:36:07 00200025 398001164A272A76
2023-11-30T20:41:18+0000        ttyUSB0
2023-11-30T20:41:34+0000        ttyUSB0 Audit on 20/6/1970 07:36:22 00200025 3880000DD8E32A76
2023-11-30T20:41:34+0000        ttyUSB0
2023-11-30T20:41:36+0000        ttyUSB0 Audit on 20/6/1970 07:36:24 00200005
2023-11-30T20:41:36+0000        ttyUSB0
2023-11-30T20:42:41+0000        ttyUSB0 Audit on 20/6/1970 07:37:29 00200016 Klajeyz
2023-11-30T20:42:41+0000        ttyUSB0
2023-11-30T20:42:41+0000        ttyUSB0 Audit on 20/6/1970 07:37:29 00200015 47800001BEAD2972
2023-11-30T20:42:41+0000        ttyUSB0
2023-11-30T20:42:41+0000        ttyUSB0 Audit on 20/6/1970 07:37:29 00200018
2023-11-30T20:42:41+0000        ttyUSB0
2023-11-30T20:43:30+0000        ttyUSB0 Audit on 20/6/1970 07:38:18 00200016 Kmrfl3b
2023-11-30T20:43:30+0000        ttyUSB0
2023-11-30T20:43:30+0000        ttyUSB0 Audit on 20/6/1970 07:38:18 00200015 3F400031F88A2A77
2023-11-30T20:43:30+0000        ttyUSB0
2023-11-30T20:43:30+0000        ttyUSB0 Audit on 20/6/1970 07:38:18 00200018
2023-11-30T20:43:30+0000        ttyUSB0
2023-11-30T20:45:09+0000        ttyUSB0 Audit on 20/6/1970 07:39:57 00200069 4780000080AD2972
2023-11-30T20:45:09+0000        ttyUSB0
2023-11-30T20:45:32+0000        ttyUSB0 Audit on 20/6/1970 07:40:20 00200069 3980011621672A76
2023-11-30T20:45:32+0000        ttyUSB0
```

ttyaudit-ttyUSB0-20231130-190131.log


```
2023-11-30T20:45:54+0000    ttyUSB0 Audit on 20/6/1970 07:40:43 00200069 478000018FED2972
2023-11-30T20:45:54+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0 TcpListener: Created IPv4 socket 20 on port 5000.
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0 TcpListener: Created IPv6 socket 21 on port 5000.
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:45:57+0000    ttyUSB0 Audit on 20/6/1970 07:40:45 00100002
2023-11-30T20:45:57+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0 TcpListener: Accepted connection on socket 22 from address 192.168.0.1.
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0 CryptoTask: Closing connection on socket 22 from address 192.168.0.1.
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:47:16+0000    ttyUSB0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2023-11-30T20:47:16+0000    ttyUSB0
2023-11-30T20:48:42+0000    ttyUSB0
2023-11-30T20:48:42+0000    ttyUSB0
2023-11-30T20:48:42+0000    ttyUSB0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2023-11-30T20:48:42+0000    ttyUSB0
2023-11-30T20:54:40+0000    ttyUSB0 Audit on 20/6/1970 07:49:28 00200069 47800000826D2972
2023-11-30T20:54:40+0000    ttyUSB0
2023-11-30T20:55:09+0000    ttyUSB0 Audit on 20/6/1970 07:49:57 00200069 47800000806D2972
2023-11-30T20:55:09+0000    ttyUSB0
2023-11-30T20:55:33+0000    ttyUSB0 Audit on 20/6/1970 07:50:22 00200069 3980011621672A76
2023-11-30T20:55:33+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0 TcpListener: Closed IPv4 socket 20 on port 5000.
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0 TcpListener: Closed IPv6 socket 21 on port 5000.
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:55:36+0000    ttyUSB0 Audit on 20/6/1970 07:50:25 00100003
2023-11-30T20:55:36+0000    ttyUSB0
2023-11-30T20:56:39+0000    ttyUSB0 Audit on 20/6/1970 07:51:27 00200023 47800000816D2972
2023-11-30T20:56:39+0000    ttyUSB0
2023-11-30T20:57:00+0000    ttyUSB0 Audit on 20/6/1970 07:51:48 00200023 3880000D4AA32A76
2023-11-30T20:57:00+0000    ttyUSB0
2023-11-30T20:57:19+0000    ttyUSB0 Audit on 20/6/1970 07:52:07 00200023 4780000081ED2972
2023-11-30T20:57:19+0000    ttyUSB0
2023-11-30T20:58:12+0000    ttyUSB0 Audit on 20/6/1970 07:53:01 0020002c 3980011654A72A76
2023-11-30T20:58:12+0000    ttyUSB0
2023-11-30T20:58:49+0000    ttyUSB0 Audit on 20/6/1970 07:53:37 0020002c 398001161F272A76
2023-11-30T20:58:49+0000    ttyUSB0
```

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.		21:29

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-202311*.log` b) `print-ttyaudit ttyaudit-tty*-202311*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**		21:32

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.**		21:33
4	CA executes the command below to display the contents of the HSMFD: `ls -ltrR`		21:33
5	CA executes the command below to set the `copy-hsmfd` script to verbose mode: `sed -i '4i set -x' /opt/icann/bin/copy-hsmfd`		21:33
6	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.**		21:40

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
7	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.**		21:14
8	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.		21:41
9	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.		21:43
10	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 # BB02638663**		21:44
11	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).		21:44

Place the Laptop into a TEB

Step	Activity	Initials	Time
12	CA places the laptop into its designated new TEB, then seals it.		21:46
13	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 # BB81420078 / Service Tag # 58SVSG2**		21:47

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
14	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: Frederico Neves** **Set # 1 TEB # BB02638669** **CO2: Pia Gruvö** **Set # 1 TEB # BB02638668** **CO4: Robert Seastrom** **Set # 1 TEB # BB02638667** **CO5: Nomsa Mwayenga** **Set # 1 TEB # BB02638666** **Set # 2 TEB # BB02638665** (CO reviews the card set prior to placing into TEB) **CO6: Hugo Salgado** **Set # 1 TEB # BB02638664**	M	22:00

CO	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO1	Set # 1 TEB # **BB02638669**	**Frederico Neves**	Frederico Neves	**2023 Nov** 30	2150	
CO2	Set # 1 TEB # **BB02638668**	**Pia Gruvö**	Pia Gruvö	**2023 Nov** 30	2152	
CO4	Set # 1 TEB # **BB02638667**	**Robert Seastrom**		**2023 Nov** 30	2154	
CO5	Set # 1 TEB # **BB02638666** Set # 2 TEB # **BB02638665**	**Nomsa Mwayenga**		**2023 Nov** 30	22:00	
CO6	Set # 1 TEB # **BB02638664**	**Hugo Salgado**		**2023 Nov** 30	22:01	

Return the Equipment to 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.)		22:03
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.**		22:04
17	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.**		22:05
18	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. **HSM5E: TEB # BB51184250** **HSM7E: TEB # BB51184251** **HSM8E: TEB # BB51184252** **Laptop4: TEB # BB81420078** **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663** **KSK-2017: TEB # BB02638662** **KSK-2023: TEB # BB02638661**		22:08

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
19	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.		22:10
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.		22:10
21	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).		22:11

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
22	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)		22:12
23	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.**		22:13
24	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.**		22:14

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

Step	Activity	Initials	Time
25	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. **Note: The COs will retrieve their new safe deposit box keys when specified below.** 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: Frederico Neves** **Box # 1239** **Set # 1 TEB # BB02638669** **CO2: Pia Gruvö** **Box # 1264** **Set # 1 TEB # BB02638668** **CO4: Robert Seastrom** **Box # 1243** **Set # 1 TEB # BB02638667** **CO5: Nomsa Mwayenga** **Box # 1262** **Set # 1 TEB # BB02638666** **Set # 2 TEB # BB02638665** **CO6: Hugo Salgado** **Box # 1242** **Set # 1 TEB # BB02638664**		

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
26	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.		
27	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.		
28	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).		

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.		22:05
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.**		22:27
3	CA reviews IW's script, then signs the participants list.		22:32
4	IW signs the list and records the completion time.		22:32

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.		22:33
6	CA requests that an SA stop the audit camera video recording.		22:33
7	CA informs onsite participants of post ceremony activities.		22:34
8	Ceremony participants take a group photo.		22:37

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.)		22:44

Bundle Audit Materials

Step	Activity	Initials	Time
10	IW makes a copy of their script for off-site audit bundle containing: a) Output of signer system - HSMFD. b) Copy of IW's key ceremony script. c) Audio-visual recording from the audit cameras. d) Logs from the Physical Access Control System and Intrusion Detection System: Range: **20230427 00:00:00 to ~~20231131~~ 20231201 00:00:00 UTC** e) IW's attestation (See Appendix C on page 51). f) SA's attestation (See Appendix D on page 52 and Appendix E on page 53). All TEBs are labeled **Root DNSSEC KSK Ceremony 51**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.		22:48

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 51.

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 52.

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

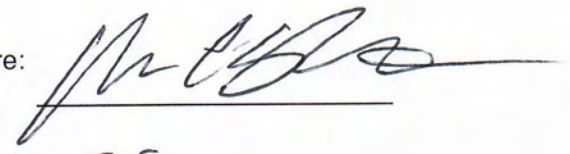
7. Other items

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: **Andy Newton**

Signature: 

Date: 2023 Nov 30

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:

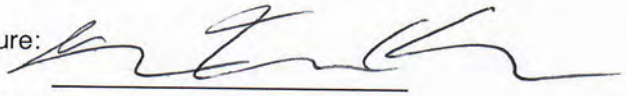
a) There were NO discrepancies found in the system configurations, assigned authorizations, and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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: **20230427 00:00:00 to 20231131 00:00:00 UTC.**

SA: Darren Kera

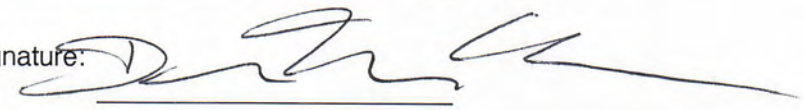
Signature: 

Date: 2023 Nov 20

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: Darren Kara

Signature: 

Date: 2023 Nov 30

```
## Last changed: 2022-05-13 15:26:15 UTC
version 19.4R3-S1.3;
system {
    host-name srx;
    root-authentication {
        encrypted-password "XXXXXXXXXX";
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user mcirilo {
            full-name "Moises D. Cirilo";
            uid 2006;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        user sfreeark {
            full-name "Sean Freeark";
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXX";
            }
        }
        password {
            format sha512;
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    domain-name ksk.cjr.dns.icann.org;
    location {
        country-code US;
        postal-code 22701;
        building Terramark-Admin;
        floor 1;
        rack 1;
    }
    ports {
        console {
            log-out-on-disconnect;
            type vt100;
        }
    }
    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;
    license {
```

```
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
chassis {
    config-button no-rescue no-clear;
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
}
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-cjr;
            }
        }
        gateway Gateway-to-KMF-West {
            ike-policy ike-policy-KMF;
            address 192.0.35.202;
            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-West {
            bind-interface st0.1;
            ike {
                gateway Gateway-to-KMF-West;
                ipsec-policy defaultPolicy;
            }
            establish-tunnels immediately;
        }
    }
    screen {
        ids-option external-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
                land;
            }
        }
    }
    nat {
        source {
            rule-set internal-to-external {
                from zone [ access guest wifi ];
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
```

```
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
policies {
    from-zone access to-zone untrust {
        policy allow-mail {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address [ icann-dns google-dns ];
                application [ junos-dns-udp junos-dns-tcp ];
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-simplex {
            match {
                source-address IDP;
                destination-address simplex;
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
    }
    from-zone access to-zone video {
        policy access-to-video {
            match {
                source-address IMS;
                destination-address kmf_east_video;
                application junos-icmp-all;
            }
            then {
                permit;
            }
        }
    }
    from-zone access to-zone ipsec {
        policy allow-access-to-ipsec {
            match {
                source-address [ ACS ACC ];
                destination-address [ kmf_west_acs kmf_west_acc ];
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-icmp {
            match {
                source-address any;
                destination-address any;
                application junos-icmp-ping;
            }
            then {
                permit;
            }
        }
        policy allow-access-access {
            match {
                source-address kmf_east_access;
                destination-address kmf_west_access;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone ipsec to-zone access {
        policy allow-ipsec-to-access {
            match {
                source-address [ kmf_west_acs kmf_west_acc ];
                destination-address [ ACS ACC ];
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-icmp {
            match {
                source-address any;
```

```
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy allow-access-access {
        match {
            source-address kmf_west_access;
            destination-address kmf_east_access;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone video to-zone ipsec {
    policy allow-video-to-ipsec {
        match {
            source-address VSS;
            destination-address kmf_west_vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_east_video;
            destination-address kmf_west_video;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone guest to-zone untrust {
    policy allow-guest-to-untrust {
        match {
            source-address kmf_east_guest;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone wifi to-zone untrust {
    policy allow-wifi-to-untrust {
        match {
            source-address kmf_east_wifi;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ipsec to-zone video {
    policy allow-ipsec-to-video {
        match {
            source-address kmf_west_vss;
            destination-address VSS;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_west_video;
            destination-address kmf_east_video;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone access to-zone access {
    policy allow-access {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
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 10.4.29.203/32;
            address ACC 10.4.29.202/32;
            address IDP 10.4.29.201/32;
            address EVM 10.4.29.200/32;
            address IMS 10.4.29.204/32;
            address E1 10.4.29.210/32;
            address E2 10.4.29.211/32;
            address E3 10.4.29.212/32;
            address E4 10.4.29.213/32;
            address kmf_east_access 10.4.29.192/26;
            address localnet 10.4.29.0/24;
            address-set iris-scanners {
                address E1;
                address E2;
                address E3;
                address E4;
            }
        }
        interfaces {
            irb.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        ntp;
                        ssh;
                    }
                }
            }
        }
    }
    security-zone untrust {
        address-book {
            address icann 192.0.32.0/20;
            address icann-dns 192.0.42.53/32;
            address googledns1 8.8.8.8/32;
            address googledns2 8.8.4.4/32;
            address simplex1 216.224.218.31/32;
            address simplex2 216.224.218.32/32;
            address simplex3 216.224.218.33/32;
            address simplex4 216.224.218.34/32;
            address-set google-dns {
                address googledns1;
                address googledns2;
            }
            address-set simplex {
                address simplex1;
                address simplex2;
                address simplex3;
                address simplex4;
            }
        }
        screen external-screen;
        interfaces {
            ge-0/0/15.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
            }
        }
    }
    security-zone video {
        address-book {
            address kmf_east_video 10.4.29.128/26;
            address VSS 10.4.29.150/32;
            address C1 10.4.29.151/32;
            address C2 10.4.29.152/32;
            address C3 10.4.29.153/32;
            address-set cameras {
                address C1;
                address C2;
                address C3;
            }
        }
        interfaces {
            irb.1 {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
            }
        }
    }
    security-zone guest {
        address-book {
            address STR 10.4.29.20/32;
            address VCC 10.4.29.22/32;
            address kmf_east_guest 10.4.29.0/25;
        }
        interfaces {
            irb.2 {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
            }
        }
    }
    security-zone ipsec {
```

```
            address-book {
                address kmf_west_access 10.4.28.192/26;
                address kmf_west_video 10.4.28.128/26;
                address kmf_west_acs 10.4.28.204/32;
                address kmf_west_acc 10.4.28.202/32;
                address kmf_west_idp 10.4.28.201/32;
                address kmf_west_evm 10.4.28.200/32;
                address kmf_west_ims 10.4.28.203/32;
                address kmf_west_E1 10.4.28.210/32;
                address kmf_west_E3 10.4.28.212/32;
                address kmf_west_E4 10.4.28.213/32;
                address kmf_west_vss 10.4.28.150/32;
                address kmf_west_C1 10.4.28.151/32;
                address kmf_west_C2 10.4.28.152/32;
                address kmf_west_C3 10.4.28.153/32;
            }
            interfaces {
                st0.1 {
                    host-inbound-traffic {
                        system-services {
                            ping;
                            ike;
                        }
                    }
                }
            }
        }
        security-zone wifi {
            address-book {
                address kmf_east_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 64.124.6.5/31;
            }
        }
    }
    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 {
            family inet {
                address 10.4.29.193/26;
            }
        }
        unit 1 {
            family inet {
                address 10.4.29.129/26;
            }
        }
        unit 2 {
            family inet {
                address 10.4.29.1/25;
            }
        }
        unit 3 {
            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 {
        10.4.29.0/24;
    }
    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 {
                        10.4.28.193/32;
                    }
                    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 64.124.6.4;
        route 10.4.28.0/24 next-hop st0.1;
        route 192.0.35.202/32 next-hop 64.124.6.4;
    }
}
```