Root DNSSEC KSK Ceremony 43

Thursday 14 October 2021

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	Matthew Larson / ICANN		2021 Oct 14	2026
IW	Patrick Jones / ICANN			
SSC1	Fernanda Iunes / ICANN			
SSC2	Joe Catapano / ICANN			
CO4	Robert Seastrom			
CO5	Christopher Griffiths			
CO6	Gaurab Upadhaya			
SA	Sean Freeark / ICANN			
SA	Darren Kara / ICANN			
RKOS / IW Backup	Aaron Foley / PTI			

By signing this script, you are declaring that this document is a true and accurate record of the Root DNSSEC KSK ceremony to the best of your knowledge, and you agree that your personal data will be processed in accordance with the ICANN Privacy Policy available at https://www.icann.org/privacy/policy

Instructions for a Root DNSSEC KSK Ceremony

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

Ceremony Guidelines:

- The CA leads the ceremony
- Only a CA, IW, or SA can enter and escort other participants into Tier 4 (Key Ceremony Room)
- Dual Occupancy is enforced. IW with CA or SA must remain inside Tier 4 (Key Ceremony Room) if participants are present in the room
- During a ceremony a CA, IW, or SA may escort participants out of Tier 4 (Key Ceremony Room) at the CA's discretion if Tier 5 (Safe Room) is not occupied
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log located in Tier 3
- The SA starts filming before the majority of participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step in order to attest to the ceremony's proper performance
- The CA reads each step aloud prior to its performance
- Upon the successful completion of a step, the IW will announce and record its time of completion, and initials that step in their script
- A ceremony participant who has cause for concern or detects an issue is encouraged to interrupt the ceremony for discussion. The issue is brought to resolution before the ceremony resumes
- Questions and suggestions for improvement are welcome and can be discussed at any time or after the ceremony during the ceremony debrief

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

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

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

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

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.	PLJ	17:00
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.	PLJ	17:01
3	CA asks that any first time ceremony participants in the room introduce themselves.	PLJ	1701
4	CA confirms that additional required personnel including COs, RZM, and Auditors are connected to the remote call. Scheduled remote participants are: **CO2: Anne-Marie Eklund Lowinder** (Key designated as backup) ✓ **RZM: Duane Wessels / Verisign** ✓ **AUD: Paul M Lee / RSM** ✓ **Note 1: The CO2 Anne-Marie Eklund Lowinder Safe Deposit Box Key TEB # BB91951321 has been designated as a backup. See Appendix F on page 43.** **Note 2: The COs' tenant key was individually transmitted to a trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.**	PLJ	1701

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
5	CA reviews emergency evacuation procedures with onsite participants.	PLJ	1702
6	CA explains the use of personal electronic devices during the ceremony.	PLJ	1702
7	CA summarizes the purpose of the ceremony.	PLJ	1702

Verify the Time and Date

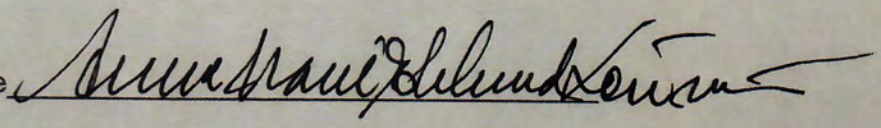
Step	Activity	Initials	Time
8	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: 2021-10-14 1703 **Note: All entries into this script or any logs should follow this common source of time.**	PLJ	1703

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with potentially less than the standard minimum of three Crypto Officers in-person, I, Anne-Marie Eklund Löwinder, am hereby entrusting my safe deposit box key enclosed in TEB # BB 9195132I for safe deposit box #1259 located within Safe #2 at the key management facility in Culpeper, VA.

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

Printed Name Anne-Marie Eklund Löwinder

Signature 

Date 2021-09-23

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
9	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)	PLJ	1704
10	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.**	PLJ	1707
11	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.	PLJ	1709

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

Step	Activity	Initials	Time
12	COs perform the following steps sequentially to retrieve the required TEBs: a) After the CA operates the guard key in the bottom lock, CO uses their tenant key to operate the top lock and open their assigned safe deposit box. b) CO reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB. c) CO reads aloud the TEB numbers, then verifies their integrity while showing them to the audit camera above. d) CO retains the TEB(s) specified below, then locks the safe deposit box. e) CO writes the date and time, then signs the safe log where **"Remove"** is indicated. f) IW verifies the completed safe log entries, then initials it. **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB46584402 (Retain)** ✓ **SO TEB # BB46584401 (Retain)** ✓ **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB46584439 (Retain)** ✓ **SO TEB # BB46584440 (Retain)** ✓ **CO6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB46584441 (Retain)** ✓ **SO TEB # BB46584442 (Retain)** ✓	PLJ	1714

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
13	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.	PLJ	1715
14	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.	PLJ	1715
15	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	PJL	1716

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
16	CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.)	PLJ	1716
17	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.**	PLJ	1718
18	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.	PLJ	1719

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

Step	Activity	Initials	Time
19	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified in the list below. d) Write the date, time, and signature on the safe log where **"Remove"** is indicated. e) IW verifies the safe log entry, then initials it. **HSM4: TEB # BB51184675 (Check and Return)** ✓ ***Last Verified: KSK Ceremony 43-AC3 2021-06-10*** **HSM5E: TEB # BB51184674 (Place on Cart)** ✓ ***Last Verified: KSK Ceremony 43-AC3 2021-06-10*** **HSM6E: TEB # BB51184245 (Place on Cart)** ✓ ***Last Verified: KSK Ceremony 43-AT 2021-10-13*** **Laptop3: TEB # BB81420111 (Check and Return)** ✓ ***Last Verified: KSK Ceremony 39 2019-11-14*** **Laptop4: TEB # BB81420106 (Place on Cart)** ✓ ***Last Verified: KSK Ceremony 37 2019-05-16*** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584443 (Place on Cart)** ✓ ***Last Verified: KSK Ceremony 39 2019-11-14*** **KSK-2017: TEB # BB46584393 (Place on Cart)** ✓ ***Last Verified: KSK Ceremony 37 2019-05-16*** **Note: *"Last verified"* indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**	PLS	1723

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

Step	Activity	Initials	Time
20	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.	PLS	1724
21	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	PLS	1725
22	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	PLS	1725

Act 2: Equipment Setup

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

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

Laptop Setup

Step	Activity	Initials	Time
1	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 # BB51184674 / Serial # H1903018** ***Last Verified: KSK Ceremony 43-AC3 2021-06-10*** **Laptop4: TEB # BB81420106 / Service Tag # 58SVSG2** ***Last Verified: KSK Ceremony 37 2019-05-16*** **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584443** ***Last Verified: KSK Ceremony 39 2019-11-14*** **Note: *"Last verified"* indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**	PLJ	1729
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.	PLJ	1729
3	CA performs the following steps to boot the laptop: a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into the serial port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Immediately insert the **OS DVD release coen-0.4.0** after the laptop power is switched ON.	PLJ	1731
4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	PLJ	1733

OS DVD Checksum Verification

Step	Activity	Initials	Time
5	CA uses the terminal window to executes the following steps: a) Calculate the SHA-256 hash by executing: `sha2wordlist < /dev/sr0` b) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash. **Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.** SHA-256 hash: **8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f** PGP Words: **minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document** **Note: The SHA-256 hash of the OS DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/43**	PLJ	1745

Printer Setup

Step	Activity	Initials	Time
6	CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page: `configure-printer`	PLJ	1745

Date Setup

Step	Activity	Initials	Time
7	CA executes `date` using the terminal window to verify if the date/time reasonably matches the ceremony clock. If the date/time do not match, perform the following steps: a) Execute `date -s "20211014 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.	PLJ	1747

Note: We paused the ceremony for a few minutes due to missing audio on live stream for YouTube. PLJ

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the **Ceremony 39 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.	PLJ	1742
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: **`hsmfd-hash -c`** CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script. **HSMFD SHA-256 HASH** 2019/11/14 `# find -P /media/HSMFD/ -type f -print0 | sort -z | xargs -0 cat | sha2wordlist` SHA-256: 51368713ada32cedea1f0c9ab34d1b30c842bc6f8e46d6467e85db2128deeb6b PGP Words: drunken congregate Neptune barbecue ringbolt pandemic Burbank unify Trojan busi nessman ammo newsletter scallion disruptive beeswax commando spaniel December showgirl hemi sphere orca detergent stockman detergent locale leprosy suspense Camelot breadline telephon e trouble Hamilton IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 39 annotated script.	PLJ	1743

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused **HSMFD 39** and the sheet of paper with the printed HSMFD hash to RKOS.	PLJ	1743

Start the Terminal Session Logging

Step	Activity	Initials	Time
11	CA executes the command below using the terminal window to change the working directory to HSMFD: **`cd /media/HSMFD`**	PLJ	1743
12	CA executes the command below to log activities of the **Commands** terminal window: **`script script-20211014.log`**	PLJ	1744

Start the HSM Activity Logging

Step	Activity	Initials	Time
13	CA performs the following steps using the **HSM Output** terminal window to capture the activity logs of the HSM: a) Change the working directory to HSMFD by executing: **`cd /media/HSMFD`** b) Set the serial port baud rate by executing: **`stty -F /dev/ttyS0 115200`** c) Start logging the serial output by executing: **`ttyaudit /dev/ttyS0`** **Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.**	PLJ	1745.

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM5E** b) Ensure an RJ45 blockout is present in the **"MGMT"** port of the HSM. Install one if not present. c) Plug the null modem cable into the serial port of the HSM. d) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H1903018**, then scroll back to the bottom. **HSM5E: Serial # H1903018** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	PBS	1746

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

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

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

Crypto Officer Credentials Check

Step	Activity	Initials	Time
1	The CA calls each of the COs listed below sequentially to perform the following steps: a) CO reads aloud the TEB number, then CA inspects it for tamper evidence. b) CO and CA open the TEB, then the CA removes the plastic case containing the card(s). c) CA opens the plastic case, then places the card(s) within on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table. **CO4: Robert Seastrom** **OP TEB # BB46584402** **SO TEB # BB46584401** **CO5: Christopher Griffiths** **OP TEB # BB46584439** **SO TEB # BB46584440** **CO6: Gaurab Upadhaya** **OP TEB # BB46584441** **SO TEB # BB46584442**	PCJ	1751

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
2	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW records which cards were used below. Each card is returned to its designated card holder after use. 1st OP card 4 of 7 2nd OP card 5 of 7 3rd OP card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCJ	1754

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.	PLJ	1754

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`
		PLJ	1755

Insert the KSRFD

Step	Activity	Initials	Time
5	CA plugs the FD labeled **"KSR"** into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window. **Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.**	PLJ	1755

Execute the KSR Signer for KSR 2022 Q1

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSR/KSK43/ksr-root-2022-q1-0.xml`	PLJ	1756
7	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	PLJ	1756

October 8, 2021

VERISIGN

To Whom It May Concern:

This is a letter of Verification of Employment for Duane Wessels. VeriSign, Inc. ("Verisign") has employed Duane Wessels full-time since January 11, 2010, currently as a Distinguished Engineer in Verisign's DNS 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 24 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,

10/8/2021

X

Dave Carney
HR Specialist - Verisign
Signed by: Carney, David

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

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

14 October 2021

The SHA256 hash of the 2022 Q1 KSR file is:

ksr-root-2022-q1-0.xml:

328944cfbed6b3dd46c6c44afd8cce31b7f8dc818b0ec2c0d0db3e234abcd2d3

The PGP wordlist for the hash above is:

PGP Words: checkup matchmaker crumpled Saturday skydive speculate scallion tambourine cubic responsive snowslide direction willow megaton spyglass company seabird warranty sweatband inventive obtuse Atlantic snapshot recipe stagnate suspicious concert cannonball dogsled pyramid standard sociable

Attested on behalf of VeriSign by:

Duane Wessels
Distinguished Engineer
DNS Operations
VeriSign, Inc.

Verify the KSR Hash for KSR 2022 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 themself. The IW verifies their employment documents and identification **off camera** for the purpose of authentication while maintaining privacy. **Note: If the RZM representative is not physically present in the room, write the representative's name and *"Remote Participant"* next to the name on the signature line.** b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line: **Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS in advance to be included in the final annotated script and audit bundle.** Duane Wessels 'Remote Participant' c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.	PVJ	1759
9	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks **"are there any objections?"**	PVJ	1800
10	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in: `/media/KSR/KSK43/skr-root-2022-q1-0.xml`	PVJ	1800

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
11	CA executes the commands below using the terminal window to print the KSR Signer log: a) `lpadmin -p HP -o copies-default=X` **Note: Replace "X" with the amount of copies needed for the participants.** b) `printlog ksrsigner-202110*.log`	PVJ	1801
12	IW attaches a copy of the required ksrsigner log to their script.	PVJ	1803

Back up the Newly Created SKR

Step	Activity	Initials	Time

13	CA executes the following commands using the terminal window:
	a) List the contents of the KSRFD by executing:
	`ls -ltrR /media/KSR`
	b) Copy the contents of the KSRFD to the HSMFD by executing:
	`cp -pR /media/KSR/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD to verify it has been copied successfully by executing:
	`ls -ltrR`
	d) Unmount the KSRFD by executing:
	`umount /media/KSR`
		PVJ	1804

14	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.**	PVJ	1804

```
Starting: ksrsigner /media/KSR/KSK43/ksr-root-2022-q1-0.xml (at Thu Oct 14 17:56:32 2021 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1903018

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-10-01T00:00:00 2021-10-22T00:00:00  26838,14748   20326(Klajeyz)/S
2  2021-10-11T00:00:00 2021-11-01T00:00:00  14748         20326(Klajeyz)/S
3  2021-10-21T00:00:00 2021-11-11T00:00:00  14748         20326(Klajeyz)/S
4  2021-10-31T00:00:00 2021-11-21T00:00:00  14748         20326(Klajeyz)/S
5  2021-11-10T00:00:00 2021-12-01T00:00:00  14748         20326(Klajeyz)/S
6  2021-11-20T00:00:00 2021-12-11T00:00:00  14748         20326(Klajeyz)/S
7  2021-11-30T00:00:00 2021-12-21T00:00:00  14748         20326(Klajeyz)/S
8  2021-12-10T00:00:00 2021-12-31T00:00:00  14748         20326(Klajeyz)/S
9  2021-12-20T00:00:00 2022-01-10T00:00:00  09799,14748   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK43/ksr-root-2022-q1-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
328944CFBED6B3DD46C6C44AFD8CCE31B7F8DC818B0EC2C0D0DB3E234ABCD2D3
>> checkup matchmaker crumpled Saturday skydive speculate scallion tambourine cubic responsive snowslide direction willow
 megaton spyglass company seabird warranty sweatband inventive obtuse Atlantic snapshot recipe stagnate suspicious concer
t cannonball dogsled pyramid standard sociable <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK43/skr-root-2022-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748   20326(Klajeyz)/S
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799         20326(Klajeyz)/S
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799         20326(Klajeyz)/S
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799         20326(Klajeyz)/S
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799         20326(Klajeyz)/S
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799         20326(Klajeyz)/S
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799         20326(Klajeyz)/S
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799         20326(Klajeyz)/S
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799   20326(Klajeyz)/S

SHA256 hash of SKR:
FD2FFA90307908A80462CBC43F94865A3FFD7E33AC8FCFF2B120D929E4CB65C7
>> willow combustion wallet millionaire chairlift inertia aimless paramount adrift gadgetry spheroid reproduce cowbell mo
lecule necklace existence cowbell Wyoming locale concurrent ribcage midsummer stagehand vagabond sailboat butterfat sugar
 certify tonic revival fracture retraction <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
15	CA deactivates the HSM by performing the following steps: **Note: CA will use OP cards not previously utilized in this ceremony if available.** a) CA displays the HSM activity logging terminal window b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"2.Set Offline"**, press **ENT** to confirm. d) When **"Set Offline?"** is displayed, press **ENT** to confirm. e) When **"Insert Card OP #X?"** is displayed, insert the OP card from the card holder. f) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. g) When **"Remove Card?"** is displayed, remove the OP card. h) Repeat steps e) to g) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **OFF.** IW records which cards were used below. Each card is returned to its designated card holder after use. 1st OP card 4 of 7 2nd OP card 5 of 7 3rd OP card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PWS	1806

Act 4: Issue Temporary CO, AAK, and SMK Cards

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

The CA will generate the required material to introduce a new HSM by performing the steps below:

- Generate CO cards for use with the cryptographic menu functions in the new HSM
- Generate AAK cards to allow the currently issued CO credentials to function in the new HSM
- Generate SMK cards to allow an existing KSK backup to be imported into the new HSM

Issue Temporary Crypto Officer (CO) Cards

Step	Activity	Initials	Time
1	CA selects the **HSM Output** terminal window.	PW	1804
2	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to issue Crypto Officer (CO) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"1.Issue Cards"**, press **ENT** to confirm. h) Select **"1.Issue CO Cards"**, press **ENT** to confirm. i) When **"Issue CO Cards?"** is displayed, press **ENT** to confirm. ✓ j) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. ✓ k) When **"Num Req Cards?"** is displayed, enter **"2"**, then press **ENT**. ✓ l) When **"Insert Card #X?"** is displayed, insert the required CO card. ✓ m) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. n) When **"Remove Card?"** is displayed, remove the CO card. o) Repeat steps l) to n) for the 2nd CO card. p) When **"CO Cards Issued"** is displayed, press **ENT** to confirm. q) Press **CLR** to return to the menu **"Role Mgmt"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st SO card 4 of 7 2nd SO card 5 of 7 3rd SO card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PLJ	1811

HSM did not ask for PIN

Issue Temporary Authorization Key (AAK) Cards

Step	Activity	Initials	Time
3	CA performs the following steps to issue Adapter Authorization Key (AAK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.Backup AAK"** from the same menu **"Role Mgmt"**, press **ENT** to confirm. c) When **"Backup AAK?"** is displayed, press **ENT** to confirm. d) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. e) When **"Insert Card #X?"** is displayed, insert the required AAK card. f) When **"Remove Card?"** is displayed, remove the AAK card. g) Repeat steps e) to f) for the 2nd AAK card. h) When **"AAK Exported"** is displayed, press **ENT** to confirm. i) Press **CLR** to return to the menu **"Secured"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCS	1813

HSM beeps "Done" AAK

Issue Temporary Storage Master Key (SMK) Cards

Step	Activity	Initials	Time
4	CA performs the following steps to issue Storage Master Key (SMK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"4.SMK"**, press **ENT** to confirm. h) Select **"2.Backup SMK"**, press **ENT** to confirm. i) When **"Backup SMK?"** is displayed, press **ENT** to confirm. j) When **"Num Cards?"** is displayed, enter **"4"**, then press **ENT**. k) When **"Num Req Cards?"** is displayed, enter **"2"**, then press **ENT**. l) When **"Insert Card #X?"** is displayed, insert the required SMK card. m) When **"Remove Card?"** is displayed, remove the SMK card. n) Repeat steps l) to m) for the 2nd, 3rd and 4th SMK cards. o) When **"Verify Card #X?"** is displayed, insert the required SMK card. p) When **"Remove Card?"** is displayed, remove the SMK card. q) Repeat steps o) to p) for the 2nd, 3rd and 4th SMK cards. r) When **"SMK Backed Up"** is displayed, press **ENT** to confirm. s) Press **CLR twice** to return to the main menu **"Secured"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCS	1819

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
5	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.**	PLJ	1820
6	CA places the HSM into a prepared TEB, then seals it.	PLJ	1822
7	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 # BB51184241 / Serial # H1903018** ✓ ✓	PLJ	1823

Act 5: 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 Secure State
- Change and verify API settings
- Import Storage Master Key (SMK)
- Import App Key
- Verify connectivity, activate, and initialize HSM
- Destroy temporary credential cards

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
1	CA performs the following steps to prepare the new HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. e) Plug the null modem cable into the serial port of the HSM. f) Connect the power to the HSM, then switch it ON. **Note: Status information should appear on the HSM activity logging screen.** g) Scroll the logging screen up and locate the HSM serial number. h) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. i) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **HSM6E: TEB # BB51184245 / Serial # H2001001** **Last Verified: KSK Ceremony 43-AT 2021-10-13** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.** **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.**	PCS	1826

Import the AAK

Step	Activity	Initials	Time
2	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. 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 the card is unreadable, gently wipe its metal contacts and try again.**	PCS	1828

Note there is an extra prompt, hit "ENT"

Configure the HSM to Secure State

Step	Activity	Initials	Time
3	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 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PL)	1831

Change the API Settings

Step	Activity	Initials	Time
4	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 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"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PW	1834

Verify API Settings

Step	Activity	Initials	Time

5	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`
		PLJ	1836

App Key Backups

Step	Activity	Initials	Time
6	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 backup HSMFD on its designated area of the ceremony table. e) Using a sharpie, write **1** and **2** respectively on the App key cards, then place them on the designated card holder. **KSK-2017: TEB # BB46584393** **Last Verified: KSK Ceremony 37 2019-05-16** **Note: *"Last verified"* indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.**	PLJ	1842

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 5 Step(s): 7 Page(s): 24 Date and Time: 2021/10/14 1851	PLS	1852
2	IW describes the exception(s) and action(s) below.	PLS	1852

In Step 7, CA had to repeat this step due to hitting CLR twice at the end, which returned the HSM to the main menu. The CA was able to repeat the step, steps Bravo through Foxtrot. At step N, CA hit CLR twice.

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 5 Step(s): 9 Page(s): 24 Date and Time: _____	PCS	1856
2	IW describes the exception(s) and action(s) below.	PCS	1856

TEB was sealed before including card holder, thus new TEB was needed.

Old TEB # BB91951367

NEW TEB # BB46584614

Import the SMK and the KSK

Step	Activity	Initials	Time
7	CA performs the following steps to import Storage Master Key (SMK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"4.SMK"**, press **ENT** to confirm. h) Select **"3.Restore SMK"**, press **ENT** to confirm. i) When **"Restore SMK?"** is displayed, press **ENT** to confirm. j) When **"Insert Card SMK #X?"** is displayed, insert the SMK card. k) When **"Remove Card?"** is displayed, remove the SMK card. l) Repeat steps j) to k) for the 2nd SMK card. m) When **"SMK Restored"** is displayed, press **ENT** to confirm. n) Press **CLR** to return to the main menu **"Key Mgmt"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PLJ	1846
8	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 same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required KSK card. g) When **"Remove Card?"** is displayed, remove the KSK card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR twice** to return to the main menu **"Secured"**. IW records which card was used below. Card is returned to its designated card holder after use. App Key card _1_ **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PLJ	1848

Return the KSK into a TEB

Step	Activity	Initials	Time
9	CA places the KSK and the backup HSMFD into a prepared TEB, then seals it.	PLJ	1845
10	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 # BB91951367**	PLJ	1854

NEW TEB # BB46584614

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
11	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert the OP card. e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. f) When **"Remove Card?"** is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **ON.** IW records which cards were used below. Each card is returned to its designated card holder after use. 1st OP card 4 of 7 2nd OP card 5 of 7 3rd OP card 4 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCJ	1900

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
12	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	PCJ	1900

13	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`
		PCJ	1901

Insert Copy of the KSRFD

Step	Activity	Initials	Time
14	CA plugs the FD labeled **"KSR_COPY"**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.**	PCJ	1903

Execute the KSR Signer for KSR 2022 Q1

Step	Activity	Initials	Time
15	CA executes the command below in the terminal window to sign the KSR file: `ksrsigner /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml`	PCJ	1903
16	When the KSR signer displays the prompt: `Activate HSM prior to accepting in the affirmative!! (y/N):` CA confirms that the HSM is online, then enters **"y"** to proceed.	PCJ	1903

```
Starting: ksrsigner /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml (at Thu Oct 14 19:03:32 2021 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H2001001

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-10-01T00:00:00 2021-10-22T00:00:00  26838,14748   20326(Klajeyz)/S
2  2021-10-11T00:00:00 2021-11-01T00:00:00  14748         20326(Klajeyz)/S
3  2021-10-21T00:00:00 2021-11-11T00:00:00  14748         20326(Klajeyz)/S
4  2021-10-31T00:00:00 2021-11-21T00:00:00  14748         20326(Klajeyz)/S
5  2021-11-10T00:00:00 2021-12-01T00:00:00  14748         20326(Klajeyz)/S
6  2021-11-20T00:00:00 2021-12-11T00:00:00  14748         20326(Klajeyz)/S
7  2021-11-30T00:00:00 2021-12-21T00:00:00  14748         20326(Klajeyz)/S
8  2021-12-10T00:00:00 2021-12-31T00:00:00  14748         20326(Klajeyz)/S
9  2021-12-20T00:00:00 2022-01-10T00:00:00  09799,14748   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799
*** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
328944CFBED6B3DD46C6C44AFD8CCE31B7F8DC818B0EC2C0D0DB3E234ABCD2D3
>> checkup matchmaker crumpled Saturday skydive speculate scallion tambourine cubic responsive snowslide direction willow
 megaton spyglass company seabird warranty sweatband inventive obtuse Atlantic snapshot recipe stagnate suspicious concer
t cannonball dogsled pyramid standard sociable <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR_COPY/KSK43/skr-root-2022-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748   20326(Klajeyz)/S
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799         20326(Klajeyz)/S
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799         20326(Klajeyz)/S
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799         20326(Klajeyz)/S
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799         20326(Klajeyz)/S
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799         20326(Klajeyz)/S
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799         20326(Klajeyz)/S
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799         20326(Klajeyz)/S
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799   20326(Klajeyz)/S

SHA256 hash of SKR:
FD2FFA90307908A80462CBC43F94865A3FFD7E33AC8FCFF2B120D929E4CB65C7
>> willow combustion wallet millionaire chairlift inertia aimless paramount adrift gadgetry spheroid reproduce cowbell mo
lecule necklace existence cowbell Wyoming locale concurrent ribcage midsummer stagehand vagabond sailboat butterfat sugar
 certify tonic revival fracture retraction <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

Verify the KSR Hash for KSR 2022 Q1

Step	Activity	Initials	Time
17	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	PCJ	1904
18	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"**	PCJ	1905
19	CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in: `/media/KSR_COPY/KSK43/skr-root-2022-q1-0.xml`	PCJ	1906

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) `lpadmin -p HP -o copies-default=X` **Note: Replace "X" with the amount of copies needed for the participants.** b) `printlog ksrsigner-202110*.log`	PCJ	1906
21	IW attaches a copy of the required ksrsigner log to their script.	PCJ	1907

Verification of the Hash of the SKR Copy

Step	Activity	Initials	Time
22	CA read the SHA256 hash in PGP wordlist format for the generated SKR and the ceremony participants match the hash with the previous SKR.	PCJ	1912

Remove Copy of the KSRFD

Step	Activity	Initials	Time

23	CA executes the following commands using the terminal window:
	a) List the contents of the KSRFD by executing:
	`ls -ltrR /media/KSR_COPY`
	b) Unmount the KSRFD by executing:
	`umount /media/KSR_COPY`
		PCJ	1913

24	CA removes the **KSR_COPY** containing the SKR files, then gives it to IW for audit purpose.	PCJ	1913

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
25	CA selects the **HSM Output** terminal window and presses the **RESTART** button on the HSM to make it offline and waits for the self test to complete. Confirm the **"READY"** LED on the HSM is **OFF**.	PCJ	1914

Clear and Destroy SMK Cards

Step	Activity	Initials	Time
26	CA performs the following steps to clear Storage Master Key (SMK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"5.Key Mgmt"**, press **ENT** to confirm. c) When **"Insert CO Card #X?"** is displayed, insert the CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select **"4.SMK"**, press **ENT** to confirm. h) Select **"4.Clear Cards"**, press **ENT** to confirm. i) When **"Clear Card?"** is displayed, press **ENT** to confirm. j) When **"Insert Card SMK 1?"** is displayed, take the **SMK #1** card from the cardholder, show the **SMK #1** card to the audit camera and then insert the **SMK #1** card into the HSM's card reader. k) When **"Num Cards?"** is displayed, enter **"4"**, then press **ENT**. l) When **"Are you sure?"** is displayed, press **ENT** to confirm. m) When **"Remove Card?"** is displayed, remove the SMK card. n) When **"Insert Card SMK #X?"** is displayed, take the **SMK #X** card from the cardholder, show the **SMK #X** card to the audit camera and then insert the **SMK #X** card into the HSM's card reader. o) When **"Are you sure?"** is displayed, press **ENT** to confirm. p) When **"Remove Card?"** is displayed, remove the SMK card. q) Repeat steps n) to p) for the 3rd and 4th SMK cards. r) Press **CLR twice** to return to the main menu **"Secured"**. s) CA uses the shredder to destroy the cleared SMK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCJ	1922

Clear and Destroy CO and AAK Cards

Step	Activity	Initials	Time
27	CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to clear Crypto Officer (CO) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"7.Role Mgmt"**, press **ENT** to confirm. c) When **"Insert Card SO #X?"** is displayed, insert the SO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd and 3rd SO card. g) Select **"4.Clear RoleCard"**, press **ENT** to confirm. h) When **"Clear Card?"** is displayed, press **ENT** to confirm. i) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. j) When **"Insert Card #X?"** is displayed, take the required **CO #X** card from the cardholder, show the **CO #X** card to the audit camera and then insert the **CO #X** card into the HSM's card reader. k) When **"Are you sure?"** is displayed, press **ENT** to confirm. l) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. m) When **"Remove Card?"** is displayed, remove the CO card. n) Repeat steps j) to m) for the 2nd CO card. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st SO card 4 of 7 2nd SO card 5 of 7 3rd SO card 6 of 7 **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCJ	~~1924~~ 1926
28	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 **"5.Clear AAK Card"** from the same menu **"Role Mgmt"**, press **ENT** to confirm. c) When **"Clear AAK Card?"** is displayed, press **ENT** to confirm. d) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**. e) 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. f) When **"Are you sure?"** is displayed, press **ENT** to confirm. g) When **"Remove Card?"** is displayed, remove the AAK card. h) Repeat steps e) to g) for the 2nd AAK card. i) Press **CLR** to return to the main menu **"Secured"**. Each card is returned to its designated card holder after use. **Note: If the card is unreadable, gently wipe its metal contacts and try again.**	PCJ	1928
29	CA uses the shredder to destroy the cleared CO and AAK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.	PCJ	1930

Temp CO 1 of 2

2 of 2

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
30	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.**	PCJ	1930
31	CA places the HSM into a prepared TEB, then seals it.	PCJ	1931
32	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. **HSM6E: TEB # BB51184242 / Serial # H2001001**	PCJ	1932

Act 6: Secure Hardware

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

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

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
1	CA performs the following steps to stop logging: a) Disconnect the null modem and ethernet cables from the laptop. b) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: i) Press `Ctrl + C` ii) Execute `exit` c) Execute the command below using the **Commands** terminal window to stop logging the terminal session: `exit` **Note: The Commands terminal session window will remain open.**	PCJ	1933

HSMFD SHA-256 HASH **2021/10/14**

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

 SHA-256:    bc486c902a47e47d3cd93ca3d90a66addec06be5a4c2e94227ff0f635409c982
PGP Words:  showgirl dictator glucose millionaire brickyard determine tonic insincere cobra
 supportive cobra pandemic sugar Apollo framework perceptive tactics recipe glitter travest
y regain repellent treadmill December brackish Yucatan artist Galveston eating applicant sp
earhead Istanbul
```

Prepare blank FDs and back up the HSMFD Contents

Step	Activity	Initials	Time
2	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: `shopt -s dotglob`	PLJ	1933
3	CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content: a) `lpadmin -p HP -o copies-default=2` b) `hsmfd-hash -p` **Note: One copy for audit bundle and one copy for HSMFD package.**	PLJ	1934
4	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrR`	PLJ	1935
5	CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs: `mkdir /media/HSMFD1`	PLJ	1935
6	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.	PLJ	1935
7	CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: `df`	PLJ	1936
8	CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD: a) `umount /dev/sdc1` b) `mkfs.vfat -n HSMFD -I /dev/sdc1` c) `mount /dev/sdc1 /media/HSMFD1` d) `cp -pR * /media/HSMFD1`	PLJ	1937
9	CA executes the commands below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy, then unmounts the flash drive before removal: a) `hsmfd-hash -m` b) `umount /media/HSMFD1`	PLJ	1937
10	CA removes the **HSMFD copy**, then places it on the holder. **Wait for the activity light on the backup HSMFD to stop flashing before removal.**	PLJ	1938
11	CA repeats step 6 to 10 for the 2nd copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	PLJ	1939
12	CA repeats step 6 to 10 for the 3rd copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	PLJ	1940
13	CA repeats step 6 to 10 for the 4th copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	PLJ	1941
14	CA repeats step 6 to 10 for the 5th copy. **Wait for the activity light on the backup HSMFD to stop flashing before executing each step.**	PLJ	1942

```
Script started on Thu Oct 14 17:44:09 2021
root@coen:/media/HSMFD# ping hsm
PING hsm (192.168.0.2) 56(84) bytes of data.
64 bytes from hsm (192.168.0.2): icmp_seq=1 ttl=255 time=0.701 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.569 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.694 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.561 ms
64 bytes from hsm (192.168.0.2): icmp_seq=5 ttl=255 time=0.570 ms
64 bytes from hsm (192.168.0.2): icmp_seq=6 ttl=255 time=0.583 ms
64 bytes from hsm (192.168.0.2): icmp_seq=7 ttl=255 time=0.565 ms
^C
--- hsm ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6149ms
rtt min/avg/max/mdev = 0.561/0.606/0.701/0.059 ms
root@coen:/media/HSMFD# ksrsigner /media/KSR/KSK43/ksr-root-2022-q1-0.xml
Starting: ksrsigner /media/KSR/KSK43/ksr-root-2022-q1-0.xml (at Thu Oct 14 17:56:32 2021
UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glib
c_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.s
o.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H1903018

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-10-01T00:00:00 2021-10-22T00:00:00  26838,14748   20326(Klajeyz)/S
2  2021-10-11T00:00:00 2021-11-01T00:00:00  14748         20326(Klajeyz)/S
3  2021-10-21T00:00:00 2021-11-11T00:00:00  14748         20326(Klajeyz)/S
4  2021-10-31T00:00:00 2021-11-21T00:00:00  14748         20326(Klajeyz)/S
5  2021-11-10T00:00:00 2021-12-01T00:00:00  14748         20326(Klajeyz)/S
6  2021-11-20T00:00:00 2021-12-11T00:00:00  14748         20326(Klajeyz)/S
7  2021-11-30T00:00:00 2021-12-21T00:00:00  14748         20326(Klajeyz)/S
8  2021-12-10T00:00:00 2021-12-31T00:00:00  14748         20326(Klajeyz)/S
9  2021-12-20T00:00:00 2022-01-10T00:00:00  09799,14748   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR/KSK43/ksr-root-2022-q1-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
328944CFBED6B3DD46C6C44AFD8CCE31B7F8DC818B0EC2C0D0DB3E234ABCD2D3
>> checkup matchmaker crumpled Saturday skydive speculate scallion tambourine cubic respo
nsive snowslide direction willow megaton spyglass company seabird warranty sweatband inve
ntive obtuse Atlantic snapshot recipe stagnate suspicious concert cannonball dogsled pyra
mid standard sociable <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK43/skr-root-2022-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748   20326(Klajeyz)/S
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799         20326(Klajeyz)/S
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799         20326(Klajeyz)/S
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799         20326(Klajeyz)/S
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799         20326(Klajeyz)/S
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799         20326(Klajeyz)/S
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799         20326(Klajeyz)/S
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799         20326(Klajeyz)/S
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799   20326(Klajeyz)/S

SHA256 hash of SKR:
FD2FFA90307908A80462CBC43F94865A3FFD7E33AC8FCFF2B120D929E4CB65C7
>> willow combustion wallet millionaire chairlift inertia aimless paramount adrift gadget
ry spheroid reproduce cowbell molecule necklace existence cowbell Wyoming locale concurre
nt ribcage midsummer stagehand vagabond sailboat butterfat sugar certify tonic revival fr
acture retraction <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20211014-175632.log **********
root@coen:/media/HSMFD# lpadmin -p HP -o copies-default=4
root@coen:/media/HSMFD# printlog ksr\007s\007igner-202110*.log
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# printlog ksrsigner-202110*.log
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /media/KSR
/media/KSR:
total 16
drwxr-xr-x 2 root root 16384 Oct 14 18:00 \033[0m\033[01;34mKSK43\033[0m

/media/KSR/KSK43:
total 144
-rw-r--r-- 1 root root 20369 Oct  2 01:53 skr.xml.20211014175632
-rw-r--r-- 1 root root 19582 Oct  2 01:53 ksr-root-2022-q1-0.xml
-rw-r--r-- 1 root root  1148 Oct  2 01:53 kskschedule.json
-rw-r--r-- 1 root root 20369 Oct 14 18:00 skr.xml
-rw-r--r-- 1 root root 20369 Oct 14 18:00 skr-root-2022-q1-0.xml
root@coen:/media/HSMFD# cp -pR /media/KSR/* .
root@coen:/media/HSMFD# ls -ltrR
.:
total 2792
-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   1493 May 16  2019 KSKSlotDB.db
-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      0 Oct 14 17:44 script-20211014.log
-rw-r--r-- 1 root root  12642 Oct 14 18:00 ttyaudit-ttyS0-20211014-174505.log
drwxr-xr-x 2 root root   8192 Oct 14 18:00 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root   6376 Oct 14 18:00 ksrsigner-20211014-175632.log
drwxr-xr-x 2 root root   8192 Oct 14 18:00 \033[01;34mKSK43\033[0m

./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

./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 Oct 14 18:00 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.3
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Oct 14 18:00 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Oct 14 18:00 skr.keybundle.0

./KSK43:
total 104
-rw-r--r-- 1 root root 20369 Oct  2 01:53 skr.xml.20211014175632
-rw-r--r-- 1 root root 19582 Oct  2 01:53 ksr-root-2022-q1-0.xml
-rw-r--r-- 1 root root  1148 Oct  2 01:53 kskschedule.json
-rw-r--r-- 1 root root 20369 Oct 14 18:00 skr.xml
-rw-r--r-- 1 root root 20369 Oct 14 18:00 skr-root-2022-q1-0.xml
root@coen:/media/HSMFD# umount /media/KSR
root@coen:/media/HSMFD# ping hsm
PING hsm (192.168.0.2) 56(84) bytes of data.
^C
--- hsm ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6145ms

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=0.882 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.479 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.687 ms
^C
--- hsm ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.479/0.682/0.882/0.167 ms
root@coen:/media/HSMFD# ksrsigner /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml
Starting: ksrsigner /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml (at Thu Oct 14 19:03:32
2021 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glib
c_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.s
o.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H2001001

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2021-10-01T00:00:00 2021-10-22T00:00:00  26838,14748   20326(Klajeyz)/S
2  2021-10-11T00:00:00 2021-11-01T00:00:00  14748         20326(Klajeyz)/S
3  2021-10-21T00:00:00 2021-11-11T00:00:00  14748         20326(Klajeyz)/S
4  2021-10-31T00:00:00 2021-11-21T00:00:00  14748         20326(Klajeyz)/S
5  2021-11-10T00:00:00 2021-12-01T00:00:00  14748         20326(Klajeyz)/S
6  2021-11-20T00:00:00 2021-12-11T00:00:00  14748         20326(Klajeyz)/S
7  2021-11-30T00:00:00 2021-12-21T00:00:00  14748         20326(Klajeyz)/S
8  2021-12-10T00:00:00 2021-12-31T00:00:00  14748         20326(Klajeyz)/S
9  2021-12-20T00:00:00 2022-01-10T00:00:00  09799,14748   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR_COPY/KSK43/ksr-root-2022-q1-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799
[warning] *** Requests signature expiration exceeds limit of 180 days! ***
...PASSED.

SHA256 hash of KSR:
328944CFBED6B3DD46C6C44AFD8CCE31B7F8DC818B0EC2C0D0DB3E234ABCD2D3
>> checkup matchmaker crumpled Saturday skydive speculate scallion tambourine cubic respo
```

```
nsive snowslide direction willow megaton spyglass company seabird warranty sweatband inve
ntive obtuse Atlantic snapshot recipe stagnate suspicious concert cannonball dogsled pyra
mid standard sociable <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR_COPY/KSK43/skr-root-2022-q1-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2022-01-01T00:00:00 2022-01-22T00:00:00  09799,14748   20326(Klajeyz)/S
2  2022-01-11T00:00:00 2022-02-01T00:00:00  09799         20326(Klajeyz)/S
3  2022-01-21T00:00:00 2022-02-11T00:00:00  09799         20326(Klajeyz)/S
4  2022-01-31T00:00:00 2022-02-21T00:00:00  09799         20326(Klajeyz)/S
5  2022-02-10T00:00:00 2022-03-03T00:00:00  09799         20326(Klajeyz)/S
6  2022-02-20T00:00:00 2022-03-13T00:00:00  09799         20326(Klajeyz)/S
7  2022-03-02T00:00:00 2022-03-23T00:00:00  09799         20326(Klajeyz)/S
8  2022-03-12T00:00:00 2022-04-02T00:00:00  09799         20326(Klajeyz)/S
9  2022-03-22T00:00:00 2022-04-12T00:00:00  47671,09799   20326(Klajeyz)/S

SHA256 hash of SKR:
FD2FFA90307908A80462CBC43F94865A3FFD7E33AC8FCFF2B120D929E4CB65C7
>> willow combustion wallet millionaire chairlift inertia aimless paramount adrift gadget
ry spheroid reproduce cowbell molecule necklace existence cowbell Wyoming locale concurre
nt ribcage midsummer stagehand vagabond sailboat butterfat sugar certify tonic revival fr
acture retraction <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20211014-190332.log **********
root@coen:/media/HSMFD# lpadmin -p HP -o copies=default=6
root@coen:/media/HSMFD# lpadmin -p HP -o copies[illegible]
root@coen:/media/HSMFD# printlog ksrsigner-202110*.log
[ 1 page * 0 copies ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltr
total 2864
-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
```

script-20211014.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   1493 May 16  2019 KSKSlotDB.db
-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 18:00 ksrsigner-20211014-175632.log
drwxr-xr-x 2 root root   8192 Oct 14 18:00 \033[01;34mKSK43\033[0m
-rw-r--r-- 1 root root  24576 Oct 14 18:03 script-20211014.log
-rw-r--r-- 1 root root  51746 Oct 14 19:05 ttyaudit-ttyS0-20211014-174505.log
drwxr-xr-x 2 root root   8192 Oct 14 19:05 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root   6391 Oct 14 19:05 ksrsigner-20211014-190332.log
root@coen:/media/HSMFD# [illegible]
\033[1@s
ksrsigner-20211014-175632.log  ksrsigner-20211014-190332.log
root@coen:/media/HSMFD# printlog ksrs\007igner-20211\007014-190332.log
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /media/KSR_COPY
/media/KSR_COPY:
total 16
drwxr-xr-x 2 root root 16384 Oct 14 19:05 \033[0m\033[01;34mKSK43\033[0m

/media/KSR_COPY/KSK43:
total 144
-rw-r--r-- 1 root root 20369 Oct  2 01:28 skr.xml.20211014190332
-rw-r--r-- 1 root root 19582 Oct  2 01:28 ksr-root-2022-q1-0.xml
-rw-r--r-- 1 root root  1148 Oct  2 01:28 kskschedule.json
-rw-r--r-- 1 root root 20369 Oct 14 19:05 skr.xml
-rw-r--r-- 1 root root 20369 Oct 14 19:05 skr-root-2022-q1-0.xml
root@coen:/media/HSMFD# umount /media/KSR_COPY
[illegible]
exit

Script done on Thu Oct 14 19:33:19 2021
```

```
2021-10-14T17:45:52+0000        ttyS0   þ
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0   H1903018 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0   BBL CRC32: 0xDBC9B9F2
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0   Running applicationBootLoader at 0xEFDC0000
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0   H1903018 011403 ABL 030 : Tamper Challenge Response Key
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:52+0000        ttyS0   ABL CRC32: 0xE7E0FA6A
2021-10-14T17:45:52+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   ####################################
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   ###     ABL tamper records       ###
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   ####################################
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   ====================================
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   vextoosTamperCount:     0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   vintoosTamperCount:     5
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   vbboosTamperCount:      0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   maxstrtempTamperCount:  0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   minstrtempTamperCount:  0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   meshTamperCount:        0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   extampSMKTamperCount:   0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   extampIMKTamperCount:   0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   tempdiffTamperCount:    0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   pfTamperCount:          5
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   restartTamperCount:     19
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   Current tamper bitmaps:
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   ======================
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
```

```
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   Bitmapped Change Record (most recent first):
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0   ========================================
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:53+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0   Running cryptoApplication at 0xEBF00000
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0   Jumping to startup @ 0x001037B4
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0   Board is P2020RDB
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0   board_smp_init: 2 cpu
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:54+0000        ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2021-10-14T17:45:54+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0   Starting next program at v0015183c
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0   Starting K-Series Kernel
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0   Copyright Ultra Electronics AEP. All Rights Reserved.
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:55+0000        ttyS0   Sat Jul  1 03:07:22 1972
2021-10-14T17:45:55+0000        ttyS0
2021-10-14T17:45:56+0000        ttyS0   Starting auditd v2.0 ... started.
2021-10-14T17:45:56+0000        ttyS0
2021-10-14T17:45:56+0000        ttyS0   Interface 0 configured for IPv6.
2021-10-14T17:45:56+0000        ttyS0
2021-10-14T17:45:56+0000        ttyS0   Interface 0 configured for IPv4.
2021-10-14T17:45:56+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   Interface 1 configured for IPv6.
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   Interface 1 configured for IPv4.
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   route: writing to routing socket: Network is unreachable
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   add net default: gateway ::: Network is unreachable
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   route: writing to routing socket: Network is unreachable
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   Starting USB driver...
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0   9860 v3.4 Keyper Application - May 19 2017 15:48:58
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0
2021-10-14T17:45:57+0000        ttyS0
```

```
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running DES POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   DES POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running Triple DES POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Triple DES POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running AES POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   AES POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running SHA1 POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   SHA1 POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running SHA2 POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   SHA2 POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running RandomGen POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   RandomGen POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running RSA POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   RSA POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running DSA POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   DSA POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running SEED POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   SEED POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running RIPEMD160 POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   RIPEMD160 POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running ECC POST Test
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   ECC POST Test Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Running HMAC POST Tests
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   HMAC POST Tests Passed
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0   Audit on 1/7/1972 03:07:25 00100008
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:45:59+0000        ttyS0
```

```
2021-10-14T17:45:59+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Keyper 9860-2  Serial Number H1903018
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Memory Usage:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   RAM (free/total)        192Mb/256Mb
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Flash (free/total)      128Mb/128Mb
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0      black store          524b
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0      statistics           112b
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0      other                116b
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   RedStore (free/total)   107Kb/128Kb
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Network Configuration:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Interface 0:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0       IPv4: enabled
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0       IPv6: enabled
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C4:9D / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c49d/64
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Interface 1:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0       IPv4: enabled
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0       IPv6: enabled
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C4:9E / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c49e/64
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   HSM Port 0: 05000
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   HSM Port 1: 03000
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Default Gateway(s): 0.0.0.0 ::
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Software Versions:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   BBL 030 ABL 021 App 034
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   CPLD Version:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   1.9
2021-10-14T17:46:00+0000        ttyS0
```

```
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   SCR Firmware Version:
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   OROS-R2.99-R1.20
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   HmcListener: Created IPv4 socket 12 on port 3000.
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   HmcListener: Created IPv6 socket 13 on port 3000.
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:46:00+0000        ttyS0   Audit on 1/7/1972 03:07:26 00100003
2021-10-14T17:46:00+0000        ttyS0
2021-10-14T17:52:22+0000        ttyS0   Audit on 1/7/1972 03:13:48 0020006a
2021-10-14T17:52:22+0000        ttyS0
2021-10-14T17:53:18+0000        ttyS0   Audit on 1/7/1972 03:14:44 00200069 0880004A83B3296D
2021-10-14T17:53:18+0000        ttyS0
2021-10-14T17:53:42+0000        ttyS0   Audit on 1/7/1972 03:15:08 00200069 0880004A7B33296D
2021-10-14T17:53:42+0000        ttyS0
2021-10-14T17:54:02+0000        ttyS0   Audit on 1/7/1972 03:15:28 00200069 0880004A7B73296D
2021-10-14T17:54:02+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0   TcpListener: Created IPv4 socket 19 on port 5000.
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0   TcpListener: Created IPv6 socket 20 on port 5000.
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:54:04+0000        ttyS0   Audit on 1/7/1972 03:15:30 00100002
2021-10-14T17:54:04+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0   TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0   CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T17:56:54+0000        ttyS0   TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2021-10-14T17:56:54+0000        ttyS0
2021-10-14T18:00:28+0000        ttyS0
2021-10-14T18:00:28+0000        ttyS0
2021-10-14T18:00:28+0000        ttyS0   CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2021-10-14T18:00:28+0000        ttyS0
2021-10-14T18:05:33+0000        ttyS0   Audit on 1/7/1972 03:26:59 00200069 0880004A83B3296D
2021-10-14T18:05:33+0000        ttyS0
2021-10-14T18:05:55+0000        ttyS0   Audit on 1/7/1972 03:27:21 00200069 0880004A7B33296D
2021-10-14T18:05:55+0000        ttyS0
2021-10-14T18:06:15+0000        ttyS0   Audit on 1/7/1972 03:27:41 00200069 0880004A7B73296D
```

```
2021-10-14T18:06:15+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0   TcpListener: Closed IPv4 socket 19 on port 5000.
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0   TcpListener: Closed IPv6 socket 20 on port 5000.
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:06:19+0000        ttyS0   Audit on 1/7/1972 03:27:45 00100003
2021-10-14T18:06:19+0000        ttyS0
2021-10-14T18:07:57+0000        ttyS0   Audit on 1/7/1972 03:29:23 00200023 00800002A48F156D
2021-10-14T18:07:57+0000        ttyS0
2021-10-14T18:08:18+0000        ttyS0   Audit on 1/7/1972 03:29:44 00200023 008000029ECF156D
2021-10-14T18:08:18+0000        ttyS0
2021-10-14T18:08:38+0000        ttyS0   Audit on 1/7/1972 03:30:04 00200023 00800002A50F156D
2021-10-14T18:08:38+0000        ttyS0
2021-10-14T18:09:36+0000        ttyS0   Audit on 1/7/1972 03:31:02 0020002f 3980011647272A76
2021-10-14T18:09:36+0000        ttyS0
2021-10-14T18:10:34+0000        ttyS0   Audit on 1/7/1972 03:32:00 0020002f 3980011646A72A76
2021-10-14T18:10:34+0000        ttyS0
2021-10-14T18:10:46+0000        ttyS0   Audit on 1/7/1972 03:32:12 00200077 3980011646A72A76
2021-10-14T18:10:46+0000        ttyS0
2021-10-14T18:12:22+0000        ttyS0   Audit on 1/7/1972 03:33:48 0020002f 398001165A272A76
2021-10-14T18:12:22+0000        ttyS0
2021-10-14T18:12:59+0000        ttyS0   Audit on 1/7/1972 03:34:25 0020002f 3980011645A72A76
2021-10-14T18:12:59+0000        ttyS0
2021-10-14T18:13:11+0000        ttyS0   Audit on 1/7/1972 03:34:37 00200010 3980011645A72A76
2021-10-14T18:13:11+0000        ttyS0
2021-10-14T18:14:38+0000        ttyS0   Audit on 1/7/1972 03:36:04 0020006b 3980011647272A76
2021-10-14T18:14:38+0000        ttyS0
2021-10-14T18:14:58+0000        ttyS0   Audit on 1/7/1972 03:36:24 0020006b 3980011646A72A76
2021-10-14T18:14:58+0000        ttyS0
2021-10-14T18:16:03+0000        ttyS0   Audit on 1/7/1972 03:37:30 0020002d 398001161AE72A76
2021-10-14T18:16:03+0000        ttyS0
2021-10-14T18:16:46+0000        ttyS0   Audit on 1/7/1972 03:38:12 0020002d 398001161A672A76
2021-10-14T18:16:46+0000        ttyS0
2021-10-14T18:17:23+0000        ttyS0   Audit on 1/7/1972 03:38:49 0020002d 3980011619E72A76
2021-10-14T18:17:23+0000        ttyS0
2021-10-14T18:18:02+0000        ttyS0   Audit on 1/7/1972 03:39:28 0020002d 398001161F672A76
2021-10-14T18:18:02+0000        ttyS0
2021-10-14T18:19:28+0000        ttyS0   Audit on 1/7/1972 03:40:54 00200007
2021-10-14T18:19:28+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0   þ
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0   H2001001 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0   BBL CRC32: 0xDBC9B9F2
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0   Running applicationBootLoader at 0xEFDC0000
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0   H2001001 011403 ABL 030 : Tamper Challenge Response Key
2021-10-14T18:25:30+0000        ttyS0
2021-10-14T18:25:30+0000        ttyS0   ABL CRC32: 0xE7E0FA6A
2021-10-14T18:25:30+0000        ttyS0
```

```
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	###################################
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	###     ABL tamper records       ###
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	###################################
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	Current Tamper Counts (decimal 0-255):
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	=====================================
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	vextoosTamperCount:     0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	vintoosTamperCount:     5
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	vbboosTamperCount:      0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	maxstrtempTamperCount:  0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	minstrtempTamperCount:  0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	meshTamperCount:        0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	extampSMKTamperCount:   0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:30+0000	ttyS0	extampIMKTamperCount:   0
2021-10-14T18:25:30+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	tempdiffTamperCount:    0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	pfTamperCount:          5
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	restartTamperCount:     17
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	Current tamper bitmaps:
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	======================
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	currentTamper bitmap:   0x0000 0b .... .... .... ....
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	Bitmapped Change Record (most recent first):
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0	=============================================
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:31+0000	ttyS0
2021-10-14T18:25:32+0000	ttyS0	Running cryptoApplication at 0xEBF00000
2021-10-14T18:25:32+0000	ttyS0
2021-10-14T18:25:32+0000	ttyS0	Jumping to startup @ 0x001037B4
2021-10-14T18:25:32+0000	ttyS0
2021-10-14T18:25:32+0000	ttyS0	Board is P2020RDB
```

```
2021-10-14T18:25:32+0000        ttyS0
2021-10-14T18:25:32+0000        ttyS0   board_smp_init: 2 cpu
2021-10-14T18:25:32+0000        ttyS0
2021-10-14T18:25:32+0000        ttyS0
2021-10-14T18:25:32+0000        ttyS0
2021-10-14T18:25:32+0000        ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2021-10-14T18:25:32+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0   Starting next program at v0015183c
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0   Starting K-Series Kernel
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0   Copyright Ultra Electronics AEP. All Rights Reserved.
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0   Sun Aug  1 06:58:31 1971
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:33+0000        ttyS0   Starting auditd v2.0 ... started.
2021-10-14T18:25:33+0000        ttyS0
2021-10-14T18:25:34+0000        ttyS0   Interface 0 configured for IPv6.
2021-10-14T18:25:34+0000        ttyS0
2021-10-14T18:25:34+0000        ttyS0   Interface 0 configured for IPv4.
2021-10-14T18:25:34+0000        ttyS0
2021-10-14T18:25:34+0000        ttyS0   Interface 1 configured for IPv6.
2021-10-14T18:25:34+0000        ttyS0
2021-10-14T18:25:34+0000        ttyS0   Interface 1 configured for IPv4.
2021-10-14T18:25:34+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0   route: writing to routing socket: Network is unreachable
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0   add net default: gateway ::: Network is unreachable
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0   route: writing to routing socket: Network is unreachable
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0   Starting USB driver...
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0   9860 v3.4 Keyper Application - May 19 2017 15:48:58
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:35+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running DES POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   DES POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running Triple DES POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Triple DES POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running AES POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   AES POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
```

```
2021-10-14T18:25:37+0000        ttyS0   Running SHA1 POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   SHA1 POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running SHA2 POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   SHA2 POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running RandomGen POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   RandomGen POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running RSA POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   RSA POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running DSA POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   DSA POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running SEED POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   SEED POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running RIPEMD160 POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   RIPEMD160 POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running ECC POST Test
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   ECC POST Test Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Running HMAC POST Tests
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   HMAC POST Tests Passed
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0   Audit on 1/8/1971 06:58:34 00100008
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:37+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Keyper 9860-2  Serial Number H2001001
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Memory Usage:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   RAM (free/total)        192Mb/256Mb
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Flash (free/total)      128Mb/128Mb
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0     black store           44b
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0     statistics            112b
```

```
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       other                116b
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   RedStore (free/total)    107Kb/128Kb
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Network Configuration:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Interface 0:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       IPv4: enabled
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       IPv6: enabled
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C7:23 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c723/64
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Interface 1:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       IPv4: enabled
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       IPv6: enabled
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C7:24 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c724/64
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   HSM Port 0: 05000
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   HSM Port 1: 03000
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Default Gateway(s): 0.0.0.0 ::
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Software Versions:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   BBL 030 ABL 021 App 034
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   CPLD Version:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   1.9
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   SCR Firmware Version:
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   OROS-R2.99-R1.20
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:25:38+0000        ttyS0   Audit on 1/8/1971 06:58:35 00100001
2021-10-14T18:25:38+0000        ttyS0
2021-10-14T18:27:30+0000        ttyS0   Audit on 1/8/1971 07:00:27 00200035 398001165A272A76
2021-10-14T18:27:30+0000        ttyS0
2021-10-14T18:27:46+0000        ttyS0   Audit on 1/8/1971 07:00:43 00200035 3980011645A72A76
2021-10-14T18:27:46+0000        ttyS0
```

```
2021-10-14T18:27:46+0000        ttyS0   Audit on 1/8/1971 07:00:43 0020000e 3980011645A72A76
2021-10-14T18:27:46+0000        ttyS0
2021-10-14T18:29:18+0000        ttyS0   Audit on 1/8/1971 07:02:15 00200023 00400000F922156D
2021-10-14T18:29:18+0000        ttyS0
2021-10-14T18:29:42+0000        ttyS0   Audit on 1/8/1971 07:02:40 00200023 00800002788F156D
2021-10-14T18:29:42+0000        ttyS0
2021-10-14T18:30:06+0000        ttyS0   Audit on 1/8/1971 07:03:03 00200023 00800002998F156D
2021-10-14T18:30:06+0000        ttyS0
2021-10-14T18:30:27+0000        ttyS0   Audit on 1/8/1971 07:03:24 00200056
2021-10-14T18:30:27+0000        ttyS0
2021-10-14T18:31:09+0000        ttyS0   Audit on 1/8/1971 07:04:06 00200081
2021-10-14T18:31:09+0000        ttyS0
2021-10-14T18:31:29+0000        ttyS0   Audit on 1/8/1971 07:04:27 00200054
2021-10-14T18:31:29+0000        ttyS0
2021-10-14T18:31:34+0000        ttyS0   Audit on 1/8/1971 07:04:32 00200028
2021-10-14T18:31:34+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   HmcListener: Created IPv4 socket 9 on port 3000.
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   HmcListener: Created IPv6 socket 11 on port 3000.
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   Audit on 1/8/1971 07:04:38 00100003
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   Audit on 1/8/1971 07:04:38 00100005
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   Shutting down daemons...
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   AuditBuffer rx'd [-1] (3)
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   shutting down audit service.
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   HmcListener::accept(): No such process
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:41+0000        ttyS0   Shutting down filesystems...
2021-10-14T18:31:41+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0   H2001001 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0   BBL CRC32: 0xDBC9B9F2
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0   Running applicationBootLoader at 0xEFDC0000
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0   H2001001 011403 ABL 030 : Tamper Challenge Response Key
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:43+0000        ttyS0   ABL CRC32: 0xE7E0FA6A
2021-10-14T18:31:43+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   ####################################
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   ###     ABL tamper records       ###
```

```
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   ####################################
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   ====================================
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   vextoosTamperCount:     0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   vintoosTamperCount:     5
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   vbboosTamperCount:      0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   maxstrtempTamperCount:  0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   minstrtempTamperCount:  0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   meshTamperCount:        0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   extampSMKTamperCount:   0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   extampIMKTamperCount:   0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   tempdiffTamperCount:    0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   pfTamperCount:          5
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   restartTamperCount:     17
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   Current tamper bitmaps:
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   ======================
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   Bitmapped Change Record (most recent first):
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0   ==========================================
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:44+0000        ttyS0
2021-10-14T18:31:45+0000        ttyS0   Running cryptoApplication at 0xEBF00000
2021-10-14T18:31:45+0000        ttyS0
2021-10-14T18:31:45+0000        ttyS0   Jumping to startup @ 0x001037B4
2021-10-14T18:31:45+0000        ttyS0
2021-10-14T18:31:45+0000        ttyS0   Board is P2020RDB
2021-10-14T18:31:45+0000        ttyS0
2021-10-14T18:31:45+0000        ttyS0   board_smp_init: 2 cpu
2021-10-14T18:31:45+0000        ttyS0
2021-10-14T18:31:45+0000        ttyS0
2021-10-14T18:31:45+0000        ttyS0
```

```
2021-10-14T18:31:45+0000	ttyS0	Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2021-10-14T18:31:45+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0	System page at phys:0000b000 user:0000b000 kern:0000b000
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0	Starting next program at v0015183c
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0	Starting K-Series Kernel
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0	Copyright Ultra Electronics AEP. All Rights Reserved.
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:46+0000	ttyS0	Sun Aug  1 07:04:44 1971
2021-10-14T18:31:46+0000	ttyS0
2021-10-14T18:31:47+0000	ttyS0	Starting auditd v2.0 ... started.
2021-10-14T18:31:47+0000	ttyS0
2021-10-14T18:31:47+0000	ttyS0	Interface 0 configured for IPv6.
2021-10-14T18:31:47+0000	ttyS0
2021-10-14T18:31:47+0000	ttyS0	Interface 0 configured for IPv4.
2021-10-14T18:31:47+0000	ttyS0
2021-10-14T18:31:47+0000	ttyS0	Interface 1 configured for IPv6.
2021-10-14T18:31:47+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	Interface 1 configured for IPv4.
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	route: writing to routing socket: Network is unreachable
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	add net default: gateway ::: Network is unreachable
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	route: writing to routing socket: Network is unreachable
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	add net default: gateway 0.0.0.0: Network is unreachable
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	Starting USB driver...
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0	9860 v3.4 Keyper Application - May 19 2017 15:48:58
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:48+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	Running DES POST Test
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	DES POST Test Passed
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	Running Triple DES POST Test
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	Triple DES POST Test Passed
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	Running AES POST Test
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	AES POST Test Passed
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	Running SHA1 POST Test
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	SHA1 POST Test Passed
2021-10-14T18:31:50+0000	ttyS0
2021-10-14T18:31:50+0000	ttyS0	Running SHA2 POST Test
```

```
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   SHA2 POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running RandomGen POST Test
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   RandomGen POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running RSA POST Test
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   RSA POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running DSA POST Test
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   DSA POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running SEED POST Test
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   SEED POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running RIPEMD160 POST Test
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   RIPEMD160 POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running ECC POST Test
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   ECC POST Test Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   Running HMAC POST Tests
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0   HMAC POST Tests Passed
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:50+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0   Keyper 9860-2  Serial Number H2001001
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0   Memory Usage:
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0   RAM (free/total)        192Mb/256Mb
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0   Flash (free/total)      128Mb/128Mb
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0      black store          272b
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0      statistics           112b
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0      other                116b
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0   RedStore (free/total)   107Kb/128Kb
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0
2021-10-14T18:31:51+0000        ttyS0
```

```
2021-10-14T18:31:51+0000	ttyS0	Network Configuration:
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	Interface 0:
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	    IPv4: enabled
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	    IPv6: enabled
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	    MAC/IP address(es): 00:E0:6C:00:C7:23 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c723/64
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	Interface 1:
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	    IPv4: enabled
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	    IPv6: enabled
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	    MAC/IP address(es): 00:E0:6C:00:C7:24 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c724/64
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	HSM Port 0: 05000
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	HSM Port 1: 03000
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	Default Gateway(s): 0.0.0.0 ::
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	Software Versions:
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	BBL 030 ABL 021 App 034
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	CPLD Version:
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	1.9
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	SCR Firmware Version:
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	OROS-R2.99-R1.20
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	HmcListener: Created IPv4 socket 9 on port 3000.
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	HmcListener: Created IPv6 socket 10 on port 3000.
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:31:51+0000	ttyS0	Audit on 1/8/1971 07:04:48 00100003
2021-10-14T18:31:51+0000	ttyS0
2021-10-14T18:32:41+0000	ttyS0	Audit on 1/8/1971 07:05:38 0020006b 3980011647272A76
2021-10-14T18:32:41+0000	ttyS0
2021-10-14T18:33:05+0000	ttyS0	Audit on 1/8/1971 07:06:02 0020006b 3980011646A72A76
```

```
2021-10-14T18:33:05+0000        ttyS0
2021-10-14T18:33:31+0000        ttyS0   Audit on 1/8/1971 07:06:28 00200039
2021-10-14T18:33:31+0000        ttyS0
2021-10-14T18:33:46+0000        ttyS0   Audit on 1/8/1971 07:06:43 0020003b
2021-10-14T18:33:46+0000        ttyS0
2021-10-14T18:34:08+0000        ttyS0   Audit on 1/8/1971 07:07:05 00200041
2021-10-14T18:34:08+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   HSM Status
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ====================
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Keyper 9860-2
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Serial Number H2001001
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Date(dd/mm/yyyy) 1/8/1971  Time 7:7:48
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Software Versions:
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   BBL 030 ABL 021 App 034
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   CPLD Version:
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   1.9
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   SCR Firmware Version:
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   OROS-R2.99-R1.20
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Memory Usage:
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   RAM (free/total)        192Mb/256Mb
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Flash (free/total)      128Mb/128Mb
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0      black store          452b
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0      statistics           112b
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0      other                116b
2021-10-14T18:34:51+0000        ttyS0
```

```
2021-10-14T18:34:51+0000	ttyS0	RedStore (free/total)   107Kb/128Kb
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0	Network Configuration:
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0	Interface 0:
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0		IPv4: enabled
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0		IPv6: enabled
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0		MAC/IP address(es): 00:E0:6C:00:C7:23 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c723/64
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0	tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			capabilities tx=0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			enabled=0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			address: 00:e0:6c:00:c7:23
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			media: Ethernet none
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			inet6 2001::2e0:6cff:fe00:c723 prefixlen 64
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			inet6 fe80::2e0:6cff:fe00:c723%tsec0 prefixlen 64 scopeid 0x2
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0	Interface 1:
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0		IPv4: enabled
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0		IPv6: enabled
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0		MAC/IP address(es): 00:E0:6C:00:C7:24 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c724/64
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0	tsec1: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			capabilities tx=0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			enabled=0
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			address: 00:e0:6c:00:c7:24
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			media: Ethernet none
2021-10-14T18:34:51+0000	ttyS0
2021-10-14T18:34:51+0000	ttyS0			inet 192.168.1.2 netmask 0xffffff00 broadcast 192.168.1.255
```

```
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0           inet6 2001::1:2e0:6cff:fe00:c724 prefixlen 64
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0           inet6 fe80::2e0:6cff:fe00:c724%tsec1 prefixlen 64 scopeid 0x3
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   HSM Port 0: 05000
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   HSM Port 1: 03000
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Default Gateway(s): 0.0.0.0 ::
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Current HSM State: Secured Off-line
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Modes: (1=Enabled 0=Disabled)
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Global Key Export    1  App Key Import       0  App Key Export       0  Asymmetric Key Gen   1
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Symmetric Key Gen    1  Symmetric Key Derive 0  Signing              1  Signature Verify     1
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   MAC Generation       1  MAC Verification     1  Encrypt / Decrypt    1  Delete Asym Key      1
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Delete Sym Key       1  Output Key Details   1  Output Key Summary   1  Suite B Algorithms   1
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Non Suite B Algs     1  Auto Online          0  Remote Management    0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Other Modes:
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   AES SMK                 Set Offline             FIPS Mode
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Battery ok
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ####################################
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ###     ABL tamper records       ###
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ####################################
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ====================================
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   vextoosTamperCount:     0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   vintoosTamperCount:     0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   vbboosTamperCount:      0
2021-10-14T18:34:51+0000        ttyS0
```

```
2021-10-14T18:34:51+0000        ttyS0   maxstrtempTamperCount:  0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   minstrtempTamperCount:  0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   meshTamperCount:        0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   extampSMKTamperCount:   0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   extampIMKTamperCount:   0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   tempdiffTamperCount:    0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   pfTamperCount:          0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   restartTamperCount:     0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Current tamper bitmaps:
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ======================
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   lastTamper bitmap:      0x0000 0b .... .... .... ....
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   Bitmapped Change Record (most recent first):
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   ========================================
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   \000====================================
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   DRBG Instantiate Health Test On Demand Passed
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   DRBG Generate Health Test On Demand Passed
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:34:51+0000        ttyS0   DRBG Reseed Health Test On Demand Passed
2021-10-14T18:34:51+0000        ttyS0
2021-10-14T18:43:09+0000        ttyS0   Audit on 1/8/1971 07:16:07 0020006b 3980011647272A76
2021-10-14T18:43:09+0000        ttyS0
2021-10-14T18:43:31+0000        ttyS0   Audit on 1/8/1971 07:16:28 0020006b 3980011646A72A76
2021-10-14T18:43:31+0000        ttyS0
2021-10-14T18:44:21+0000        ttyS0   Audit on 1/8/1971 07:17:18 00200025 398001161AE72A76
2021-10-14T18:44:21+0000        ttyS0
2021-10-14T18:44:39+0000        ttyS0   Audit on 1/8/1971 07:17:36 00200025 398001161A672A76
2021-10-14T18:44:39+0000        ttyS0
2021-10-14T18:44:41+0000        ttyS0   Audit on 1/8/1971 07:17:38 00200005
2021-10-14T18:44:41+0000        ttyS0
2021-10-14T18:46:00+0000        ttyS0   Audit on 1/8/1971 07:18:58 0020006b 3980011647272A76
```

```
2021-10-14T18:46:00+0000        ttyS0
2021-10-14T18:46:20+0000        ttyS0   Audit on 1/8/1971 07:19:17 0020006b 3980011646A72A76
2021-10-14T18:46:20+0000        ttyS0
2021-10-14T18:47:47+0000        ttyS0   Audit on 1/8/1971 07:20:44 00200016 Klajeyz
2021-10-14T18:47:47+0000        ttyS0
2021-10-14T18:47:47+0000        ttyS0   Audit on 1/8/1971 07:20:44 00200015 4780000180AD2972
2021-10-14T18:47:47+0000        ttyS0
2021-10-14T18:47:47+0000        ttyS0   Audit on 1/8/1971 07:20:44 00200018
2021-10-14T18:47:47+0000        ttyS0
2021-10-14T18:59:12+0000        ttyS0   Audit on 1/8/1971 07:32:09 00200069 0880004A83B3296D
2021-10-14T18:59:12+0000        ttyS0
2021-10-14T18:59:33+0000        ttyS0   Audit on 1/8/1971 07:32:30 00200069 0880004A7B33296D
2021-10-14T18:59:33+0000        ttyS0
2021-10-14T18:59:44+0000        ttyS0   Audit on 1/8/1971 07:32:41 0020006a
2021-10-14T18:59:44+0000        ttyS0
2021-10-14T19:00:16+0000        ttyS0   Audit on 1/8/1971 07:33:13 00200069 0880004A7B73296D
2021-10-14T19:00:16+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0   TcpListener: Created IPv4 socket 20 on port 5000.
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0   TcpListener: Created IPv6 socket 21 on port 5000.
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:00:18+0000        ttyS0   Audit on 1/8/1971 07:33:15 00100002
2021-10-14T19:00:18+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0   TcpListener: Accepted connection on socket 22 from address 192.168.0.1.
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0   CryptoTask: Closing connection on socket 22 from address 192.168.0.1.
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:03:47+0000        ttyS0   TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2021-10-14T19:03:47+0000        ttyS0
2021-10-14T19:05:56+0000        ttyS0
2021-10-14T19:05:56+0000        ttyS0
2021-10-14T19:05:56+0000        ttyS0   CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2021-10-14T19:05:56+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   H2001001 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   BBL CRC32: 0xDBC9B9F2
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   Running applicationBootLoader at 0xEFDC0000
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   H2001001 011403 ABL 030 : Tamper Challenge Response Key
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ABL CRC32: 0xE7E0FA6A
2021-10-14T19:14:17+0000        ttyS0
```

```
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ###################################
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ###     ABL tamper records       ###
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ###################################
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ====================================
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   vextoosTamperCount:     0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   vintoosTamperCount:     5
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   vbboosTamperCount:      0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   maxstrtempTamperCount:  0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   minstrtempTamperCount:  0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   meshTamperCount:        0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   extampSMKTamperCount:   0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   extampIMKTamperCount:   0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   tempdiffTamperCount:    0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   pfTamperCount:          5
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   restartTamperCount:     19
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   Current tamper bitmaps:
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ======================
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   Bitmapped Change Record (most recent first):
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0   ============================================
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:17+0000        ttyS0
2021-10-14T19:14:18+0000        ttyS0   Running cryptoApplication at 0xEBF00000
2021-10-14T19:14:18+0000        ttyS0
2021-10-14T19:14:18+0000        ttyS0   Jumping to startup @ 0x001037B4
2021-10-14T19:14:18+0000        ttyS0
2021-10-14T19:14:18+0000        ttyS0   Board is P2020RDB
```

```
2021-10-14T19:14:18+0000	ttyS0
2021-10-14T19:14:18+0000	ttyS0	board_smp_init: 2 cpu
2021-10-14T19:14:18+0000	ttyS0
2021-10-14T19:14:18+0000	ttyS0
2021-10-14T19:14:18+0000	ttyS0
2021-10-14T19:14:18+0000	ttyS0	Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2021-10-14T19:14:18+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	System page at phys:0000b000 user:0000b000 kern:0000b000
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	Starting next program at v0015183c
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	Starting K-Series Kernel
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	Copyright Ultra Electronics AEP. All Rights Reserved.
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	Sun Aug  1 07:47:18 1971
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	Starting auditd v2.0 ... started.
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:20+0000	ttyS0	Interface 0 configured for IPv6.
2021-10-14T19:14:20+0000	ttyS0
2021-10-14T19:14:21+0000	ttyS0	Interface 0 configured for IPv4.
2021-10-14T19:14:21+0000	ttyS0
2021-10-14T19:14:21+0000	ttyS0	Interface 1 configured for IPv6.
2021-10-14T19:14:21+0000	ttyS0
2021-10-14T19:14:21+0000	ttyS0	Interface 1 configured for IPv4.
2021-10-14T19:14:21+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0	route: writing to routing socket: Network is unreachable
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0	add net default: gateway ::: Network is unreachable
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0	route: writing to routing socket: Network is unreachable
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0	add net default: gateway 0.0.0.0: Network is unreachable
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0	Starting USB driver...
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0	9860 v3.4 Keyper Application - May 19 2017 15:48:58
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:22+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0	Running DES POST Test
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0	DES POST Test Passed
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0	Running Triple DES POST Test
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0	Triple DES POST Test Passed
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0	Running AES POST Test
2021-10-14T19:14:23+0000	ttyS0
2021-10-14T19:14:23+0000	ttyS0	AES POST Test Passed
2021-10-14T19:14:23+0000	ttyS0
```

```
2021-10-14T19:14:23+0000        ttyS0   Running SHA1 POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   SHA1 POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running SHA2 POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   SHA2 POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running RandomGen POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   RandomGen POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running RSA POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   RSA POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running DSA POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   DSA POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running SEED POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   SEED POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running RIPEMD160 POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   RIPEMD160 POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running ECC POST Test
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   ECC POST Test Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   Running HMAC POST Tests
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:23+0000        ttyS0   HMAC POST Tests Passed
2021-10-14T19:14:23+0000        ttyS0
2021-10-14T19:14:24+0000        ttyS0   Audit on 1/8/1971 07:47:21 00100008
2021-10-14T19:14:24+0000        ttyS0
2021-10-14T19:14:24+0000        ttyS0
2021-10-14T19:14:24+0000        ttyS0
2021-10-14T19:14:24+0000        ttyS0
2021-10-14T19:14:24+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Keyper 9860-2  Serial Number H2001001
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Memory Usage:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   RAM (free/total)        192Mb/256Mb
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Flash (free/total)      128Mb/128Mb
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0      black store          524b
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0      statistics           112b
```

```
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       other                116b
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   RedStore (free/total)    107Kb/128Kb
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Network Configuration:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Interface 0:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       IPv4: enabled
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       IPv6: enabled
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C7:23 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c723/64
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Interface 1:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       IPv4: enabled
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       IPv6: enabled
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C7:24 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c724/64
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   HSM Port 0: 05000
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   HSM Port 1: 03000
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Default Gateway(s): 0.0.0.0 ::
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Software Versions:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   BBL 030 ABL 021 App 034
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   CPLD Version:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   1.9
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   SCR Firmware Version:
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   OROS-R2.99-R1.20
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   HmcListener: Created IPv4 socket 12 on port 3000.
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0
```

```
2021-10-14T19:14:25+0000        ttyS0   HmcListener: Created IPv6 socket 13 on port 3000.
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:14:25+0000        ttyS0   Audit on 1/8/1971 07:47:23 00100003
2021-10-14T19:14:25+0000        ttyS0
2021-10-14T19:15:41+0000        ttyS0   Audit on 1/8/1971 07:48:38 0020006b 3980011647272A76
2021-10-14T19:15:41+0000        ttyS0
2021-10-14T19:16:04+0000        ttyS0   Audit on 1/8/1971 07:49:02 0020006b 3980011646A72A76
2021-10-14T19:16:04+0000        ttyS0
2021-10-14T19:17:43+0000        ttyS0   Audit on 1/8/1971 07:50:41 0020002d 398001161AE72A76
2021-10-14T19:17:43+0000        ttyS0
2021-10-14T19:18:46+0000        ttyS0   Audit on 1/8/1971 07:51:44 0020002d 398001161A672A76
2021-10-14T19:18:46+0000        ttyS0
2021-10-14T19:19:29+0000        ttyS0   Audit on 1/8/1971 07:52:26 0020002d 3980011619E72A76
2021-10-14T19:19:29+0000        ttyS0
2021-10-14T19:20:09+0000        ttyS0   Audit on 1/8/1971 07:53:07 0020002d 398001161F672A76
2021-10-14T19:20:09+0000        ttyS0
2021-10-14T19:23:42+0000        ttyS0   Audit on 1/8/1971 07:56:40 00200023 00800002A48F156D
2021-10-14T19:23:42+0000        ttyS0
2021-10-14T19:23:59+0000        ttyS0   Audit on 1/8/1971 07:56:57 00200023 008000029ECF156D
2021-10-14T19:23:59+0000        ttyS0
2021-10-14T19:24:19+0000        ttyS0   Audit on 1/8/1971 07:57:16 00200023 00800002A50F156D
2021-10-14T19:24:19+0000        ttyS0
2021-10-14T19:25:44+0000        ttyS0   Audit on 1/8/1971 07:58:42 00200070 3980011647272A76
2021-10-14T19:25:44+0000        ttyS0
2021-10-14T19:26:35+0000        ttyS0   Audit on 1/8/1971 07:59:33 00200070 3980011646A72A76
2021-10-14T19:26:35+0000        ttyS0
2021-10-14T19:27:54+0000        ttyS0   Audit on 1/8/1971 08:00:52 0020002c 398001165A272A76
2021-10-14T19:27:54+0000        ttyS0
2021-10-14T19:28:35+0000        ttyS0   Audit on 1/8/1971 08:01:33 0020002c 3980011645A72A76
2021-10-14T19:28:35+0000        ttyS0
```

Print Logging Information

Step	Activity	Initials	Time
15	CA executes the following commands using the terminal window to print a copy of the logging information: a) `lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true` b) `enscript -2Gr script-202110*.log` c) `enscript -Gr --font="Courier8" ttyaudit-tty*-202110*.log` Attach the printed copies to IW script. **Note: Ignore the error regarding non-printable characters if prompted.**	PLJ	1945

Place HSMFDs and OS DVDs into a TEB

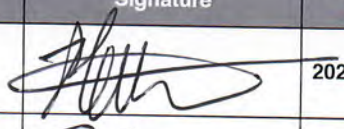
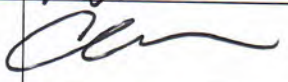
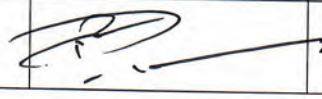
Step	Activity	Initials	Time
16	CA executes the following commands using the terminal window to unmount the HSMFD: a) `cd /tmp` b) `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder.	PLJ	1946
17	CA performs the following steps to switch OFF the laptop and remove the OS DVD: a) Remove the OS DVD from the laptop. b) Turn OFF the laptop by pressing the power button. c) Disconnect all connections from the laptop.	PLJ	1947
18	CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it.	PLJ	1948
19	CA performs the following steps to verify the TEB: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS DVD TEB on the cart. **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951368**	PLJ	1948
20	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	PLJ	1949

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.	PCJ	1950
22	CA performs the following steps: a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and laptop serial number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the laptop TEB on the cart. **Laptop4: TEB # BB81420124 / Service Tag # 58SVSG2**	PCJ	1951

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
23	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps: a) CA takes the OP TEB and plastic case prepared for the CO. b) CO takes their OP card from the card holder and places it inside the plastic case. c) CO gives the plastic case containing the OP card to the CA. d) CA places the plastic case into the prepared TEB, reads aloud the TEB number and description, then seals it. e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony inventory. f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. g) CA gives the TEB containing the card to the CO. h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. i) Repeat steps a) to h) for the 2 SO cards respectively, ensuring they're facing outward in the plastic case and placed into the prepared SO TEB. j) CO writes the date and time, then signs the table of IW's script, then IW initials the entry. k) CO returns to their seat with their credentials, being especially careful not to compromise any TEB. l) Repeat steps for all the remaining COs on the list. **CO4: Robert Seastrom** **OP TEB # BB91951237** **SO TEB # BB91951236** **CO5: Christopher Griffiths** **OP TEB # BB91951235** **SO TEB # BB91951234** **CO6: Gaurab Upadhaya** **OP TEB # BB91951233** **SO TEB # BB91951232**	PCJ	2000

CO	Card Type	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO4	OP 4 of 7 SO 4 of 7	OP TEB # BB91951237 SO TEB # BB91951236	Robert Seastrom		2021 Oct 14	20:01	PJ
CO5	OP 5 of 7 SO 5 of 7	OP TEB # BB91951235 SO TEB # BB91951234	Christopher Griffiths		2021 Oct 14	20:01	JG
CO6	OP 6 of 7 SO 6 of 7	OP TEB # BB91951233 SO TEB # BB91951232	Gaurab Upadhaya		2021 Oct 14	20:01	PJ

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

Step	Activity	Initials	Time
24	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)	PLS	2002
25	SSC1 opens Safe #1 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.**	PLS	2003
26	SSC1 removes the safe log, then writes the date and time, then signs the safe log where **"Open Safe"** is indicated. IW verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PLS	2004
27	CA performs the following steps to return each piece of equipment to the safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where **"Return"** is indicated. d) IW verifies the safe log entry, then initials it. **HSM5E: TEB # BB51184241** ✓ **HSM6E: TEB # BB51184242** ✓ **Laptop4: TEB # BB81420124** ✓ **OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951368** ✓ **KSK-2017: ~~TEB # BB91951367~~** BB4658461 4	PLS	2008

Page 34

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
28	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.	PLS	2009
29	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	PLS	2010
30	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	PLS	2010

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
31	CA and IW transport a flashlight, and escort SSC2 and the COs into Tier 5 (Safe Room.)	PLS	2011
32	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.**	PLS	2012
33	SSC2 removes the safe log, then writes the date and time, then signs the safe log where **"Open Safe"** is indicated. IW verifies this entry, then initials it. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PLS	2012

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

Step	Activity	Initials	Time
34	COs perform the following steps sequentially to return the required TEBs: a) CO reads aloud the TEB number(s), then verifies integrity while showing the TEB(s) to the audit camera above b) After the CA operates the guard key in the bottom lock, CO uses their tenant key to operate the top lock and open their safe deposit box. c) CO reads aloud the safe deposit box number, places their TEB(s) inside, then locks the safe deposit box. 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. **CO4: Robert Seastrom** **Box # 1260** **OP TEB # BB91951237** ✓ **SO TEB # BB91951236** ✓ **CO5: Christopher Griffiths** **Box # 1240** **OP TEB # BB91951235** ✓ **SO TEB # BB91951234** **CO6: Gaurab Upadhaya** **Box # 1261** **OP TEB # BB91951233** ✓ **SO TEB # BB91951232** ✓	PLJ	2018

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
35	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry, then initials it.	PLJ	2019
36	SSC2 returns the safe log back to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	PLJ	2020
37	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	PLJ	2020

Act 7: 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.	PLS	2024
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.**	PLS	2028
3	CA reviews IW's script, then signs the participants list.	PLS	2031
4	IW signs the list and records the completion time.	PLS	2031

Stop Online Streaming and Post Ceremony Information

Step	Activity	Initials	Time
5	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.	PLS	2031
6	CA informs onsite participants of post ceremony activities.	PLS	2032
7	Ceremony participants take a group photo.	PLS	2033

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

Step	Activity	Initials	Time
8	RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.) SA, IW, and CA must remain in Tier 4 (Key Ceremony Room.)	PLS	2035
9	CA requests that an SA stop the audit camera video recording.	PLS	2035

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: **20191114 00:00:00 to 20211015 00:00:00 UTC** e) IW's attestation (See Appendix C on page 40). f) SA's attestation (See Appendix D on page 41 and Appendix E on page 42). All TEBs are labeled **Root DNSSEC KSK Ceremony 43**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	PLS	21:30

Appendix A: References

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

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

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

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

[4] **`hsmfd-hash:`** Is a bash script used to calculate, print and compare SHA-256 checksums for the HSMFD flash drives. It has the following options:

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

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

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

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

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

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

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

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

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

[9] **`keybackup:`** Is an application written in C by Dr. Richard Lamb, which list, delete, and backup keys.
The source code is available at https://github.com/iana-org/dnssec-keytools

---

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

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes during the ceremony and attestation. See Appendix C on page 40.

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 41.

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 42. 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: **Patrick Jones**

Signature: Patrick Jones

Date: 2021 Oct 14

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: **20191114 00:00:00 to 20211015 00:00:00 UTC.**

SA: Darren Kara

Signature:

Date: 2021 Oct 14

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

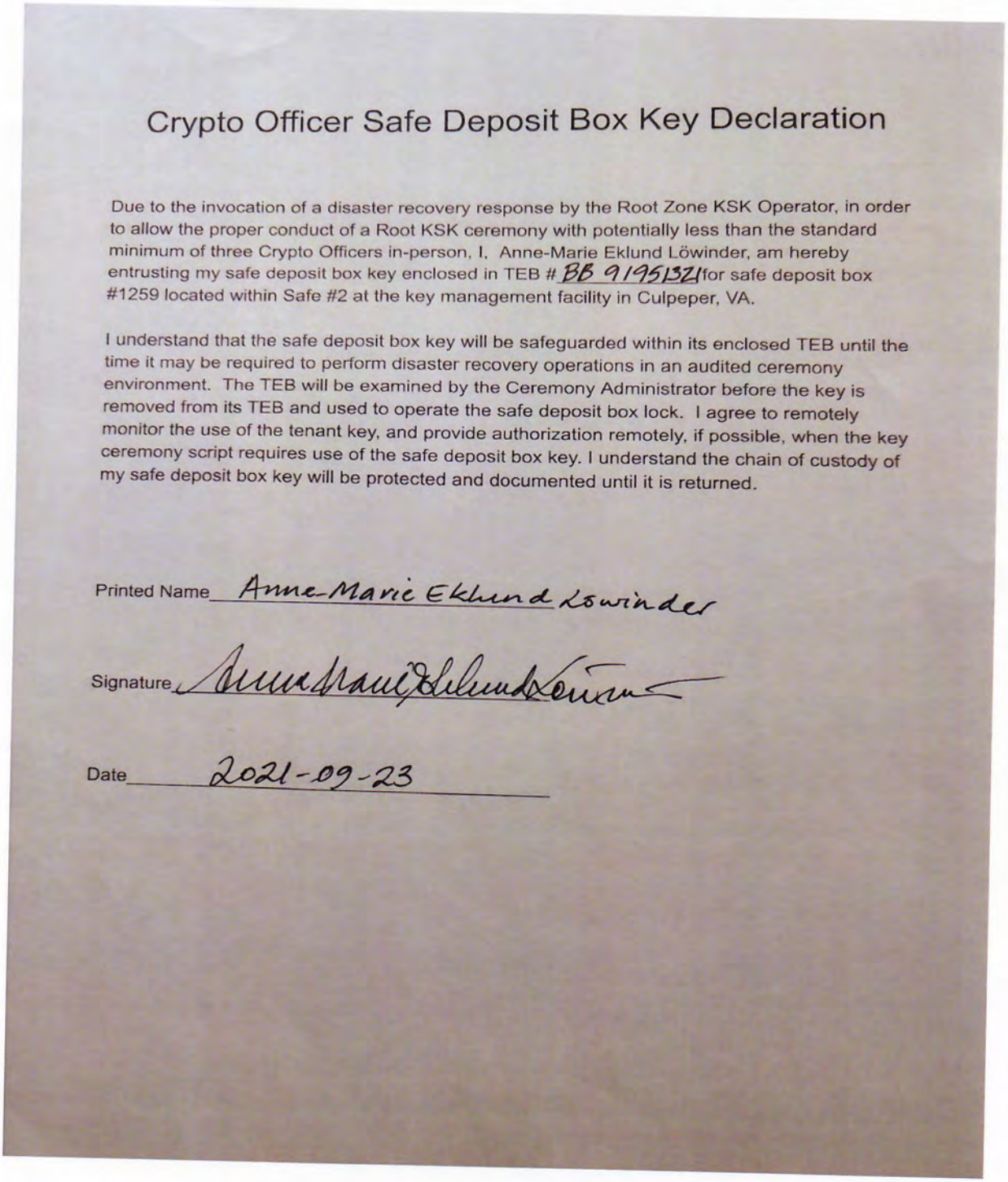
Signature:

Date: 2021 Oct 14

Appendix F: CO2 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO2 Anne-Marie Eklund Lowinder** Safe Deposit Box **Key TEB #BB91951321** dispatched from the CO.

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



Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with potentially less than the standard minimum of three Crypto Officers in-person, I, Anne-Marie Eklund Löwinder, am hereby entrusting my safe deposit box key enclosed in TEB # BB 91951321 for safe deposit box #1259 located within Safe #2 at the key management facility in Culpeper, VA.

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

Printed Name Anne-Marie Eklund Löwinder

Signature

Date 2021-09-23

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Anne-Marie Eklund Löwinder** hereby attest that my safe deposit box key for safe deposit box **#1259** located within Safe #2 at the key management facility in Culpeper, VA, USA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951321** before transmitting the key via courier.

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

Printed Name Anne-Marie Eklund Löwinder

Signature Anne-Marie Eklund Löwinder

Date 25 October 2021

```
## Last commit: 2021-10-15 15:14:03 UTC by root
version 15.1X49-D170.4;
system {
    host-name srx;
    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;
        }
    }
    root-authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
    }
    name-server {
        192.0.42.53;
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        user sfreeark {
            full-name "Sean Freeark";
            uid 2002;
```

```
            class super-user;
            authentication {
                encrypted-password "XXXXXXXXXXXXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
            }
        }
        password {
            format sha512;
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    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;
        }
    }
}
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;
    }
}
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;
```