# Root DNSSEC KSK Ceremony 48

Wednesday 01 February 2023

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

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

## 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 | ~~James Mitchell~~ / PTI | | 2023 Feb 02 | ~~21:09~~ 02:23 |
| IW | Jonathan Denison / ICANN | | | |
| SSC1 | Sabrina Tanamal / PTI | | | |
| SSC2 | Hilary Jin / ICANN | | | |
| CO1 | Arbogast Fabian | | | |
| CO2 | Ralf Weber | | | |
| CO3 | João Damas | | | |
| CO4 | Carlos Martinez | | | |
| CO5 | Ólafur Guðmundsson | | | |
| CO6 | Jorge Etges | | | |
| CO7 | Subramanian Moonesamy | | | |
| RZM | Duane Wessels / Verisign | | | |
| RZM | Poonam Garg / Verisign | | | |
| AUD | Emmanuel Nkereuwem / RSM | | | |
| AUD | John Leonard / RSM | | | |
| SA | Patrick Tudor / ICANN | | | |
| SA | Josh Jenkins / ICANN | | | |
| RKOS / CA Backup | Andres Pavez / PTI | | | |
| RKOS / IW Backup | Aaron Foley / PTI | | | |
| EW | Alex Boyd | | | |
| | | | | |
| | | | | |
| | | | | |

***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 |

# Root DNSSEC Script Exception

## Exception Details

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | IW writes the details of the ceremony exception:<br>Act: 1 Step(s): 2 Page(s): 5<br>Date and Time: 01-02-2023 21:01<br>**Note: IW describes the exception(s) and action(s) below.** | JD | 21:01 |

JAMES MITCHELL UNAVAILABLE AS CA DUE TO EXTENUATING CIRCUMSTANCES.
REPLACED BY GUSTAVO LOZANO.

# 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' cards required to operate the HSM

## Sign into Tier 4 (Key Ceremony Room)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | CA confirms with SA that all audit cameras are recording and online video streaming is enabled. | JD | 21:01 |
| 2 | CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2. | JD | 21:03 |
| 3 | CA asks that any first time ceremony participants in the room introduce themselves. | JD | 21:04 |

## Emergency Evacuation Procedures and Electronics Policy

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4 | CA reviews emergency evacuation procedures with onsite participants. | JD | 21:04 |
| 5 | CA explains the use of personal electronic devices during the ceremony. | JD | 21:05 |
| 6 | CA summarizes the purpose of the ceremony. | JD | 21:06 |

## Verify the Time and Date

| Step | Activity | Initials | Time |
|---|---|---|---|
| 7 | IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room):<br><br>Date and time: 01-02-2023 21:06<br><br>**Note: All entries into this script or any logs should follow this common source of time.** | JD | 21:06 |

# Open Safe #2 (Tier 6, Credentials Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 8 | CA transports the guard key and flashlight, and with IW escorts SSC2 and the COs into Tier 5 (Safe Room.) | JD | 21:08 |
| 9 | SSC2 opens Safe #2 while shielding the combination from the camera.<br>**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.** | JD | 21:09 |
| 10 | Perform the following steps to complete the safe log:<br>a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera.<br>b) IW provides the pre-printed safe log to SSC2.<br>c) SSC2 writes the date and time, then signs the safe log where **"Open Safe"** is indicated.<br>d) IW verifies the entry then initials it. | JD | 21:10 |

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

| Step | Activity | Initials | Time |
|---|---|---|---|
| 11 | COs perform the following steps sequentially to access the listed TEBs:<br>a) After the CA operates the guard key in the bottom lock, CO reads aloud their safe deposit box number then uses their tenant key to operate the top lock.<br>b) CO opens their safe deposit box, verifies its integrity, then removes the TEBs.<br>c) CO reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above.<br>d) CO performs the actions specified blow, then locks their safe deposit box.<br>**Note 1: The CO's key will remain inserted in their assigned safe deposit box lock when specified below.**<br>**Note 2: The COs will retrieve their new safe deposit box keys when specified below.**<br>e) CO writes the date and time, then signs the safe log.<br>f) IW verifies the completed safe log entries, then initials them.<br><br>**CO1: Arbogast Fabian**<br>**Box # 1788**<br>**OP TEB # BB91951310** (Check and Return)<br>**SO TEB # BB91951309** (Check and Return)<br><br>**CO2: Ralf Weber**<br>**Box # 1071**<br>**OP TEB # BB46584378** (Retain)<br>**SO TEB # BB46584379** (Retain)<br><br>**CO3: João Damas**<br>**Box # 1069**<br>**OP TEB # BB91951308** (Check and Return)<br>**SO TEB # BB91951307** (Check and Return)<br><br>**CO4: Carlos Martinez**<br>**Box # 1791** (Key shall remain in lock)<br>**New Box # 1073** (Retrieve keys from lock)<br>**OP TEB # BB91951257** (Transfer to newly assigned safe deposit box)<br>**SO TEB # BB91951254** (Retain)<br><br>**CO5: Ólafur Guðmundsson**<br>**Box # 1789** (Key shall remain in lock)<br>**New Box # 1070** (Retrieve keys from lock)<br>**OP TEB # BB91951256** (Transfer to newly assigned safe deposit box)<br>**SO TEB # BB91951253** (Retain)<br><br>**CO6: Jorge Etges**<br>**Box # 1072**<br>**OP TEB # BB91951306** (Check and Return)<br>**SO TEB # BB91951305** (Check and Return)<br><br>**CO7: Subramanian Moonesamy**<br>**Box # 1790**<br>**OP TEB # BB91951304** (Check and Return)<br>**SO TEB # BB91951303** (Check and Return) | JD | 21:29 |

## Close Safe #2 (Tier 6, Credentials Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 12 | Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry then initials it. | JD | 21:30 |
| 13 | SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off. | JD | 21:31 |
| 14 | CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room). | JD | 21:31 |

## Open Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 15 | CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.) | JD | 21:33 |
| 16 | SSC1 opens Safe #1 while shielding the combination from the camera.<br>**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.** | JD | 21:34 |
| 17 | Perform the following steps to complete the safe log:<br>a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera.<br>b) IW provides the pre-printed safe log to SSC1.<br>c) SSC1 writes the date and time, then signs the safe log where **"Open Safe"** is indicated.<br>d) IW verifies the entry then initials it. | JD | 21:35 |

# Root DNSSEC Script Exception

## Exception Details

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | IW writes the details of the ceremony exception:<br>Act: 1 Step(s): 18 Page(s): 9<br>Date and Time: 01-02-2023 21:41<br>**Note: IW describes the exception(s) and action(s) below.** | JD | 21:41 |

AS GUSTAVO LOZANO REPLACED JAMES MITCHELL AS CA, THE NAME IN LOG FILES FOR SAFE #2 WERE UPDATED BY HAND TO REFLECT THE CHANGE.

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

| Step | Activity | Initials | Time |
|---|---|---|---|
| 18 | CA performs the following steps to extract each piece of equipment from the safe:<br>a) CAREFULLY remove each equipment TEB from the safe.<br>b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera.<br>c) Place each equipment TEB on the cart as specified in the list below.<br>d) Write the date and time, then signs the safe log.<br>e) IW verifies the completed safe log entries, then initials it.<br><br>**HSM5W: TEB # BB51184248 (Check and Return)**<br>Last Verified: KSK Ceremony 46 2022-08-17<br>**HSM6W: TEB # BB51184288 (Place on Cart)**<br>Last Verified: KSK Ceremony 44 2022-02-16<br>**HSM7W: TEB # BB51184544 (Place on Cart)**<br>Last Verified: AT Ceremony 48 2023-01-31<br><br>**Laptop3: TEB # BB81420073 (Place on Cart)**<br>Last Verified: KSK Ceremony 44 2022-02-16<br>**Laptop4: TEB # BB81420086 (Check and Return)**<br>Last Verified: KSK Ceremony 46 2022-08-17<br><br>**OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951311 (Place on Cart)**<br>Last Verified: KSK Ceremony 46 2022-08-17<br><br>**KSK-2017: TEB # BB91951258 (Place on Cart)**<br>Last Verified: KSK Ceremony 44 2022-02-16<br><br>**Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.** | JD | 21:41 |

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

| Step | Activity | Initials | Time |
|---|---|---|---|
| 19 | SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry then initials it. | JD | 21:42 |
| 20 | SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off. | JD | 21:42 |
| 21 | CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room). | JD | 21:43 |

# 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:<br>a) Remove all equipment TEBs from the cart and place them on the ceremony table.<br>b) Inspect each equipment TEB for tamper evidence.<br>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.<br>d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.<br><br>**HSM6W: TEB # BB51184288 / Serial # H2008009**<br>Last Verified: KSK Ceremony 44 2022-02-16<br>**Laptop3: TEB # BB81420073 / Service Tag # C8SVSG2**<br>Last Verified: KSK Ceremony 44 2022-02-16<br>**OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951311**<br>Last Verified: KSK Ceremony 46 2022-08-17<br><br>**Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.** | JD | 21:49 |
| 2 | CA performs the following steps to confirm that no hard drive and battery are in the laptop:<br>a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty.<br>b) Open the latch on the left side of the laptop to confirm that the battery slot is empty. | JD | 21:50 |
| 3 | CA performs the following steps to boot the laptop:<br>a) Connect the USB printer cable into the rear USB port of the laptop.<br>b) Connect the null modem cable into the serial port of the laptop.<br>c) Connect the external HDMI display cable.<br>d) Connect the power supply.<br>e) Immediately insert the **OS DVD release coen-0.4.0** after the laptop power is switched ON. | JD | 21:52 |
| 4 | CA verifies functionality of the external display and performs adjustments if necessary:<br>To change the font size of the terminal:<br>Click the **View** menu and select **Zoom In** or **Zoom Out**<br>To change the resolution of each screen:<br>Go to **Applications > Settings > Display** | JD | 21:54 |

## OS DVD Checksum Verification

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5 | CA uses the terminal window to executes the following steps:<br>a) Calculate the SHA-256 hash by executing:<br>`sha2wordlist < /dev/sr0`<br>b) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.<br>**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.**<br><br>SHA-256 hash:<br>**8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f**<br>PGP Words:<br>**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**<br><br>**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/48** | JD | 21:57 |

## 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:<br>`configure-printer` | JD | 21:57 |

## 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.<br><br>If the date/time do not match, perform the following steps:<br>a) Execute `date -s "20230201 HH:MM:00"` to set the time.<br>**where `HH` is two-digit hour, `MM` is two-digit minutes and `00` is zero seconds.**<br>b) Execute `date` to confirm the date/time matches the clock. | JD | 21:58 |

## Connect the HSMFD

| Step | Activity | Initials | Time |
|---|---|---|---|
| 8 | CA plugs the **Ceremony 46 HSMFD** into the USB slot, then performs the steps below:<br>a) Wait for the OS to recognize it.<br>b) Display the HSMFD contents to all participants.<br>c) Close the file system window. | JD | 22:00 |
| 9 | CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD:<br>`hsmfd-hash -c`<br>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.<br>**HSMFD SHA-256 HASH** 2022/08/17<br>`# find -P /media/HSMFD/ -type f -print0 \| sort -z \| xargs -0 cat \| sha2wordlist`<br>SHA-256: a0f857fa4b5f1ff61ba5beaa4eba247798753d100dbb3b4a2aa65ecab78e2e31<br>PGP Words: ragtime warranty eightball whimsical dragnet forever billiard vocalist beeswax paperweight skydive pedigree drifter puberty bluebird inception printer impartial commence autopsy ancient publisher clockwork direction brickyard paragon eyeglass revenue seabird mi crowave buzzard company<br>IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 46 annotated script. | JD | 22:01 |

## Distribute Previous HSMFD

| Step | Activity | Initials | Time |
|---|---|---|---|
| 10 | CA gives the unused **HSMFD 46** and the sheet of paper with the printed HSMFD hash to RKOS. | JD | 22:01 |

## 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:<br>`cd /media/HSMFD` | JD | 22:02 |
| 12 | CA executes the command below to log activities of the **Commands** terminal window:<br>`script script-20230201.log` | JD | 22:02 |

## 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:<br>a) Change the working directory to HSMFD by executing:<br>`cd /media/HSMFD`<br>b) Set the serial port baud rate by executing:<br>`stty -F /dev/ttyS0 115200`<br>c) Start logging the serial output by executing:<br>`ttyaudit /dev/ttyS0`<br>**Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.** | JD | 22:03 |

# Power ON the HSM (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 14 | CA performs the following steps to prepare the HSM:<br>a) Verify the label on the HSM reads **HSM6W**.<br>b) Plug the null modem cable into the serial port of the HSM.<br>c) Connect the power to the HSM, then switch it ON.<br>**Note: Status information should appear on the HSM activity logging screen.**<br>d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads **H2008009**.<br>e) Scroll down to the end of the logging screen.<br><br>**HSM6W: Serial # H2008009**<br>**Note: The date and time on the HSM is not used as a reference for logging and timestamp.** | JD | 22:05 |

# Act 3: Reissue COs' Cards

The CA will generate all of the COs' cards by performing the steps below:

- Generate Crypto Officer (CO) cards used to access the key management functions in the HSM. Required for adding or deleting keys stored in an HSM
- Generate Operator (OP) cards to configure the HSM to an online or offline state and facilitate communication through the ethernet adapter. Required for communication with the laptop for key signing operations
- Generate temporary Adapter Authorization Key (AAK) cards to configure an HSM to use existing OP, CO, and SO cards previously generated in an HSM
- Generate Storage Master Key (SMK) cards to allow an HSM to read an encrypted APP key backup. Required for migrating keys and disaster recovery operations

## Crypto Officer Credentials Verification

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | The CA calls each of the COs listed below sequentially to perform the following steps:<br>a) CO reads aloud the TEB number, then CA inspects it for tamper evidence.<br>b) CO and CA open the TEB, then the CA removes the plastic case containing the card(s).<br>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.<br><br>**CO2: Ralf Weber**<br>**OP TEB # BB46584378**<br>**SO TEB # BB46584379**<br><br>**CO4: Carlos Martinez**<br>**SO TEB # BB91951254**<br><br>**CO5: Ólafur Guðmundsson**<br>**SO TEB # BB91951253** | JD | 22:10 |

# Issue Two Sets of Crypto Officer (CO) Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2 | CA selects the **HSM Output** terminal window. | JD | 22:10 |
| 3 | 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:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"7.Role Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert Card SO #X?"** is displayed, insert the SO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the SO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd SO card.<br>g) Select **"1.Issue Cards"**, press **ENT** to confirm.<br>h) Select **"1.Issue CO Cards"**, press **ENT** to confirm.<br>i) When **"Issue CO Cards?"** is displayed, press **ENT** to confirm.<br>j) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**.<br>k) When **"Num Req Cards?"** is displayed, enter **"3"**, then press **ENT**.<br>l) When **"Insert Card #X?"** is displayed, insert the required CO card.<br>m) When **"Remove Card?"** is displayed, remove the CO card.<br>n) Repeat steps l) to m) until all the CO cards have been issued.<br>o) When **"CO Cards Issued"** is displayed, press **ENT** to confirm.<br>p) Repeat steps h) to o) to create a **2nd CO card set**.<br><br>IW records which cards were used below. Each card is returned to its designated card holder after use.<br>Set # 2<br>1st SO card 2 of 7<br>2nd SO card 4 of 7<br>3rd SO card 5 of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.**<br>**Note: The default PIN for a new card is set as 11223344.** | JD | 22:25 |

## Issue Two Sets of Operator (OP) Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4 | CA performs the following steps to issue Operator (OP) Cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"2.Issue OP Cards** from the current **"1.Issue Cards"** menu, then press **ENT** to confirm.<br>c) When **"Issue OP Cards?"** is displayed, press **ENT** to confirm.<br>d) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**.<br>e) When **"Num Req Cards?"** is displayed, enter **"3"**, then press **ENT**.<br>f) When **"Insert Card #X?"** is displayed, insert the required OP card.<br>g) When **"Remove Card?"** is displayed, remove the OP card.<br>h) Repeat steps f) to g) until all the OP cards have been issued.<br>i) When **"OP Cards Issued"** is displayed, press **ENT** to confirm.<br><br>j) Repeat steps b) to i) to create a **2nd OP card set**.<br><br>k) Press **CLR** to return to the menu **"Role Mgmt"**.<br><br>Each card is returned to its designated card holder after use.<br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.**<br>**Note: The default PIN for a new card is set as 11223344.** | JD | 22:36 |

## Issue Temporary Adapter Authorization Key (AAK) Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5 | CA performs the following steps to issue temporary Adapter Authorization Key (AAK) cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"3.Backup AAK"** from the current **"Role Mgmt"** menu, then press **ENT** to confirm.<br>c) When **"Backup AAK?"** is displayed, press **ENT** to confirm.<br>d) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**.<br>e) When **"Insert Card #X?"** is displayed, insert the required AAK card.<br>f) When **"Remove Card?"** is displayed, remove the AAK card.<br>g) Repeat steps e) to f) for the 2nd AAK card.<br>h) When **"Done AAK"** is displayed, press **ENT** to confirm.<br>i) Press **CLR** to return to the menu **"Secured"**.<br><br>Each card is returned to its designated card holder after use.<br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 22:38 |

# Test the CO Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 6 | CA performs the following steps to test the CO cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"5.Key Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert CO Card #X?"** is displayed, insert the CO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the CO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd CO card.<br>g) Press **CLR** to return to the menu **"Secured"**.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st CO card **7** of 7<br>2nd CO card **6** of 7<br>3rd CO card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 22:41 |
| 7 | CA repeats step 6 using the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st CO card **4** of 7<br>2nd CO card **3** of 7<br>3rd CO card **2** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 22:43 |
| 8 | CA repeats step 6 using the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st CO card **3** of 7<br>2nd CO card **2** of 7<br>3rd CO card **1** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 22:45 |

# Issue Two Sets of Storage Master Key (SMK) Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 9 | CA performs the following steps to issue Storage Master Key (SMK) cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"5.Key Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert CO Card #X?"** is displayed, insert the CO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the CO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd CO card.<br><br>g) Select **"4.SMK"**, press **ENT** to confirm.<br>h) Select **"2.Backup SMK"**, press **ENT** to confirm.<br>i) When **"Backup SMK?"** is displayed, press **ENT** to confirm.<br>j) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**.<br>k) When **"Num Req Cards?"** is displayed, enter **"3"**, then press **ENT**.<br>l) When **"Insert Card #X?"** is displayed, insert the required SMK card.<br>m) When **"Remove Card?"** is displayed, remove the SMK card.<br>n) Repeat steps l) to m) until all the SMK cards have been issued.<br>o) When **"Verify Card #X?"** is displayed, insert the required SMK card.<br>p) When **"Remove Card?"** is displayed, remove the SMK card.<br>q) Repeat steps o) to p) until all the SMK cards have been verified.<br>r) When **"SMK Backed Up"** is displayed, press **ENT** to confirm.<br><br>s) Repeat steps h) to r) to create a **2nd SMK card set**.<br><br>t) Press **CLR twice** to return to the main menu **"Secured"**.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st CO card **7** of 7<br>2nd CO card **6** of 7<br>3rd CO card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | CJD | 23:03 |

# Test the OP Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 10 | CA performs the following steps to test the OP cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"1.Set Online"**, press **ENT** to confirm.<br>c) When **"Set Online?"** is displayed, press **ENT** to confirm.<br>d) When **"Insert Card OP #X?"** is displayed, insert the OP card.<br>e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>f) When **"Remove Card?"** is displayed, remove the OP card.<br>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **ON.**<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st OP card **7** of 7<br>2nd OP card **6** of 7<br>3rd OP card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 23:05 |
| 11 | CA performs the following steps to test the OP cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"2.Set Offline"**, press **ENT** to confirm.<br>c) When **"Set Offline?"** is displayed, press **ENT** to confirm.<br>d) When **"Insert Card OP #X?"** is displayed, insert the OP card from the card holder.<br>e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>f) When **"Remove Card?"** is displayed, remove the OP card.<br>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **OFF.**<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st OP card **4** of 7<br>2nd OP card **3** of 7<br>3rd OP card **2** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 23:07 |

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

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

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

## Enable/Activate the HSM (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | CA performs the following steps to activate the HSM:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"1.Set Online"**, press **ENT** to confirm.<br>c) When **"Set Online?"** is displayed, press **ENT** to confirm.<br>d) When **"Insert Card OP #X?"** is displayed, insert the OP card.<br>e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>f) When **"Remove Card?"** is displayed, remove the OP card.<br>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **ON.**<br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st OP card **3** of 7<br>2nd OP card **2** of 7<br>3rd OP card **1** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 23:09 |

## Check the Network Connectivity Between Laptop and HSM

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2 | CA connects the HSM to the laptop using an ethernet cable in the LAN ports. | JD | 23:09 |
| 3 | CA performs the following steps to test the network connectivity between laptop and HSM:<br>a) Use the **Commands** terminal window<br>b) Test connectivity by executing:<br>`ping hsm`<br>c) Wait for responses, then exit by pressing:<br>`Ctrl + C` | JD | 23:10 |

## Insert the KSRFD

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4 | CA plugs the **KSRFD** into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window.<br><br>**Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.** | JD | 23:11 |

January 18, 2023

VERISIGN

To Whom It May Concern:

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

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

For more than 25 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 163.7 million .com and .net domain names and processing more than 219 billion query transactions daily-keeping the world connected online, seamlessly and securely. Verisign is experienced in and provides support for both IPv6 and DNSSEC.

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

Sincerely,

X Dave Carney January 18, 2023

Dave Carney
HR Specialist - Verisign

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

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

1 February 2023

The SHA256 hash of the 2023 Q2 KSR file is:

**ksr-root-2023-q2-0.xml:**

5fd01e5ad586cd76544f7a6948c2b5dd7c51837f59e13e62bf0e76288ee982cb

The PGP wordlist for the hash above is:

**PGP Words:** eyetooth savagery berserk existence sterling letterhead spindle impetus eating document keyboard guitarist deadbolt repellent scorecard tambourine kiwi enchanting Mohawk integrate endow tolerance concert gadgetry slingshot Atlantic inverse cellulose orca ultimate miser revival

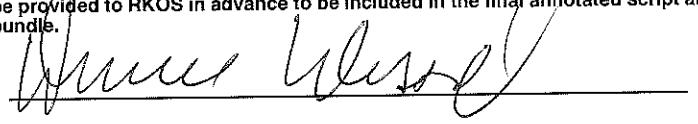
Attested on behalf of Verisign by:

Duane Wessels
Fellow
Naming Operations
Verisign, Inc.

## Execute the KSR Signer for KSR 2023 Q2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5 | CA executes the command below in the terminal window to sign the KSR file:<br>`ksrsigner /media/KSRFD/KSK48/ksr-root-2023-q2-0.xml` | JD | 23:11 |
| 6 | When the KSR signer displays the prompt:<br>`Activate HSM prior to accepting in the affirmative!! (y/N):`<br>CA confirms that the HSM is online, then enters **"y"** to proceed. | JD | 23:12 |

## Verify the KSR Hash for KSR 2023 Q2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 7 | When the hash of the KSR is displayed in the terminal window, perform the following:<br>a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification **off camera** for the purpose of authentication while maintaining privacy.<br>**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.**<br>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:<br>**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.**<br>  <br>c) The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used. | JD | 23:14 |
| 8 | Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"** | JD | 23:14 |
| 9 | CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in:<br>`/media/KSRFD/KSK48/skr-root-2023-q2-0.xml` | JD | 23:15 |

## Print Copies of the KSR Signer Log

| Step | Activity | Initials | Time |
|---|---|---|---|
| 10 | CA executes the commands below using the terminal window to print the KSR Signer log:<br>a) `lpadmin -p HP -o copies-default=X`<br>**Note: Replace "X" with the amount of copies needed for the participants.**<br>b) `printlog ksrsigner-202302*.log` | JD | 23:17 |
| 11 | IW attaches a copy of the required ksrsigner log to their script. | JD | 23:17 |

```
Starting: ksrsigner /media/KSRFD/KSK48/ksr-root-2023-q2-0.xml (at Wed Feb  1 23:11:51 2023 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H2008009

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-01-01T00:00:00 2023-01-22T00:00:00  18733,00951   20326(Klajeyz)/S
2  2023-01-11T00:00:00 2023-02-01T00:00:00  00951         20326(Klajeyz)/S
3  2023-01-21T00:00:00 2023-02-11T00:00:00  00951         20326(Klajeyz)/S
4  2023-01-31T00:00:00 2023-02-21T00:00:00  00951         20326(Klajeyz)/S
5  2023-02-10T00:00:00 2023-03-03T00:00:00  00951         20326(Klajeyz)/S
6  2023-02-20T00:00:00 2023-03-13T00:00:00  00951         20326(Klajeyz)/S
7  2023-03-02T00:00:00 2023-03-23T00:00:00  00951         20326(Klajeyz)/S
8  2023-03-12T00:00:00 2023-04-02T00:00:00  00951         20326(Klajeyz)/S
9  2023-03-22T00:00:00 2023-04-12T00:00:00  00951,60955   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSRFD/KSK48/ksr-root-2023-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  60955,00951
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955
...PASSED.

SHA256 hash of KSR:
5FD01E5AD586CD76544F7A6948C2B5DD7C51837F59E13E62BF0E76288EE982CB
>> eyetooth savagery berserk existence sterling letterhead spindle impetus eating document keyboard guitarist deadbolt re
pellent scorecard tambourine kiwi enchanting Mohawk integrate endow tolerance concert gadgetry slingshot Atlantic inverse
 cellulose orca ultimate miser revival <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSRFD/KSK48/skr-root-2023-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  00951,60955   20326(Klajeyz)/S
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955         20326(Klajeyz)/S
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955         20326(Klajeyz)/S
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955         20326(Klajeyz)/S
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955         20326(Klajeyz)/S
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955         20326(Klajeyz)/S
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955         20326(Klajeyz)/S
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955         20326(Klajeyz)/S
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955   20326(Klajeyz)/S

SHA256 hash of SKR:
13E107A29EEF9D818FC20CBDC8EFB1661CED9B280677B1C2308973C50BBB5CA9
>> Aztec tolerance ahead Pacific quiver unravel quadrant inventive payday repellent ammo quantity spaniel unravel sailboa
t gossamer befriend unify puppy cellulose afflict inception sailboat repellent chairlift matchmaker hockey resistor alone
 publisher escape passenger <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

## Back up the Newly Created SKR

| Step | Activity | Initials | Time |
|---|---|---|---|
| 12 | CA executes the following commands using the terminal window:<br>a) List the contents of the KSRFD by executing:<br>`ls -ltrR /media/KSRFD`<br>b) Copy the contents of the KSRFD to the HSMFD by executing:<br>`cp -pR /media/KSRFD/* .`<br>**Note: Confirm overwrite by entering "y" if prompted.**<br>c) List the contents of the HSMFD to verify it has been copied successfully by executing:<br>`ls -ltrR`<br>d) Calculate the SKR SHA-256 hash by executing:<br>`sha2wordlist < KSK48/skr-root-2023-q2-0.xml`<br>e) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash from the KSR Signer log.<br>f) Unmount the KSRFD by executing:<br>`umount /media/KSRFD` | JD | 23:20 |
| 13 | CA removes the **KSRFD** containing the SKR files, then gives it to the RZM representative.<br>**Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.** | JD | 23:20 |

## Disable/Deactivate the HSM (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 14 | CA deactivates the HSM by performing the following steps:<br>**Note: CA will use OP cards not previously utilized in this ceremony if available.**<br>a) CA displays the HSM activity logging terminal window<br>b) Utilize the HSM's keyboard to scroll through the menu using < ><br>c) Select **"2.Set Offline"**, press **ENT** to confirm.<br>d) When **"Set Offline?"** is displayed, press **ENT** to confirm.<br>e) When **"Insert Card OP #X?"** is displayed, insert the OP card from the card holder.<br>f) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>g) When **"Remove Card?"** is displayed, remove the OP card.<br>h) Repeat steps d) to f) for the 2nd and 3rd OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **OFF.**<br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st OP card **7** of 7<br>2nd OP card **6** of 7<br>3rd OP card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 23:22 |

## Place the HSM (Tier 7) into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 15 | CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.<br>**Note: DO NOT unplug the cable connections on the laptop.** | JD | 23:23 |
| 16 | CA places the HSM into its designated new TEB, then seals it. | JP | 23:24 |
| 17 | CA performs the following steps:<br>a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number and HSM serial number match below.<br>c) Initial the TEB along with IW using a ballpoint pen.<br>d) Give IW the sealing strips for post-ceremony inventory.<br>e) Place the HSM TEB on the cart.<br><br>**HSM6W: TEB # BB51184545 / Serial # H2008009** | JD | 23:25 |

## Ceremony Break

| Step | Activity | Initials | Time |
|---|---|---|---|
| 18 | CA divides the participants who desire a ceremony break into groups and ensures the following:<br>a) Remaining participants are sufficient to maintain dual occupancy guidelines for the ceremony room.<br>b) Audit Cameras are never obstructed.<br><br>RKOS will escort each group of participants out of the ceremony room for the ceremony break. | JD | 23:51 |
| 19 | Once all of the groups have returned to Tier 4 (Ceremony Room) from the break, CA ensures that all participants are present and resumes the ceremony. | JD | 23:52 |

# Act 5: Issue SO Cards and Introduce New HSM

The CA will issue SO Cards and introduce a new HSM by performing the following steps:

- Verify new HSM serial number
- Import the Adapter Authorization Key (AAK)
- Generate Security Officer (SO) cards to perform HSM administrative operations. Required to create other role cards (OP and CO), and the introduction and zeroization of an HSM
- Configure the HSM to a secure state
- Change and verify API settings
- Import Storage Master Key (SMK)
- Import App Key (KSK)
- Verify connectivity, activate, and initialize HSM
- Destroy temporary AAK cards

## Power ON the HSM (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | CA selects the **HSM Output** terminal window. | JD | 23:53 |
| 2 | CA performs the following steps to prepare the new HSM:<br>a) Remove the TEB from the cart and place it on the ceremony table.<br>b) Inspect the TEB for tamper evidence.<br>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.<br>d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.<br>e) Plug the null modem cable into the serial port of the HSM.<br>f) Connect the power to the HSM, then switch it ON.<br>**Note: Status information should appear on the HSM activity logging screen.**<br>g) Scroll the logging screen up and locate the HSM serial number.<br>h) IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom.<br>i) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state.<br><br>**HSM7W: TEB # BB51184544 / Serial # H2110017**<br>Last Verified: AT Ceremony 48 2023-01-31<br>**Note: The date and time on the HSM is not used as a reference for logging and timestamp.**<br><br>**Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.** | JD | 23:56 |

# Root DNSSEC Script Exception

## Exception Details

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | IW writes the details of the ceremony exception:<br>Act: 5 Step(s): 4(g) Page(s): 25<br>Date and Time: 01-02-2023 23:59<br>**Note: IW describes the exception(s) and action(s) below.** | JD | 23:59 |

SCRIPT INDICATES A PROMPT SHOULD DISPLAY THAT REQUESTS A PIN, HOWEVER, NO REQUEST IS MADE/DISPLAYED. PROCESS CONTINUES WITHOUT ENTERING PIN, AS IT IS ASSUMED IT WILL UTILIZE DEFAULT PIN.

# Import the AAK

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3 | CA performs the following steps to import the Adapter Authorization Key (AAK):<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"2.Restore AAK"**, press **ENT** to confirm.<br>c) When **"Restore AAK?"** is displayed, press **ENT** to confirm.<br>d) When **"Insert Card #X?"** is displayed, insert the required AAK card and press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the AAK card.<br>f) Repeat steps d) to e) for the 2nd AAK card.<br>g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm.<br><br>Each card is returned to its designated card holder after use.<br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 23:57 |

# Issue Two Sets of Security Officer (SO) Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 4 | CA performs the following steps to issue Security Officer (SO) Cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"1.Issue SO Cards**, press **ENT** to confirm.<br>c) When **"Issue SO Cards?"** is displayed, press **ENT** to confirm.<br>d) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**.<br>e) When **"Num Req Cards?"** is displayed, enter **"3"**, then press **ENT**.<br>f) When **"Insert Card #X?"** is displayed, insert the required SO card.<br>g) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>h) When **"Remove Card?"** is displayed, remove the SO card.<br>i) Repeat steps f) to h) until all the SO cards have been issued.<br>j) When **"SO Cards Issued"** is displayed, press **ENT** to confirm.<br><br>k) Repeat steps b) to j) to create a **2nd SO cards set**.<br><br>Each card is returned to its designated card holder after use.<br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:09 |

# Configure the HSM to Secure State

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5 | CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"3.Secure"**, press **ENT** to confirm.<br>c) When **"Secure?"** is displayed, press **ENT** to confirm.<br>d) When **"Insert Card SO #X?"** is displayed, insert the SO card.<br>e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>f) When **"Remove Card?"** is displayed, remove the SO card.<br>g) Repeat steps d) to f) for the 2nd and 3rd SO cards.<br>h) When **"SMK AES Triple DES?"** is displayed, press **CLR** to skip.<br>i) When **"SMK AES"** is displayed, press **ENT** to confirm.<br>j) When **"LAN Port Number?"** is displayed, press **CLR** to skip.<br>k) When **"Enable IPv4/IPv6?"** is displayed, press **CLR** to skip.<br>l) When **"LAN IPv4 Address?"** is displayed, press **CLR** to skip.<br>m) When **"LAN IPv4 Mask?"** is displayed, press **CLR** to skip.<br>n) When **"Set IPv4 Gateway?"** is displayed, press **CLR** to skip.<br>o) When **"LAN IPv6 Address?"** is displayed, press **CLR** to skip.<br>p) When **"LAN IPv6 Mask?"** is displayed, press **CLR** to skip.<br>q) When **"Set IPv6 Gateway?"** is displayed, press **CLR** to skip.<br>r) When **"Remote Mgmt Off Enable?"** is displayed, press **CLR** to skip.<br>s) When **"Remote Mgmt Off** is displayed, press **ENT** to confirm.<br>t) When **"Change Clock?"** is displayed, press **CLR** to skip.<br>u) When **"Import Config?"** is displayed, press **CLR** to skip.<br>v) When **"FIPS Mode On Disable?"** is displayed, press **CLR** to skip.<br>w) When **"FIPS Mode On"** is displayed, press **ENT** to confirm.<br>x) When **"Global Key Export Enabled"** is displayed, press **CLR** to skip.<br><br>**Done Rebooting Device** will be displayed.<br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st SO card **7** of 7<br>2nd SO card **6** of 7<br>3rd SO card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:12 |

# Test the SO Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 6 | CA performs the following steps to test the SO cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"7.Role Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert Card SO #X?"** is displayed, insert the SO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the SO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd SO card.<br>g) Press **CLR** to return to the menu **"Secured"**.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st SO card **4** of 7<br>2nd SO card **3** of 7<br>3rd SO card **2** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:14 |
| 7 | CA repeats step 6 using the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st SO card **3** of 7<br>2nd SO card **2** of 7<br>3rd SO card **1** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:15 |
| 8 | CA repeats step 6 using the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st SO card **7** of 7<br>2nd SO card **6** of 7<br>3rd SO card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:17 |
| 9 | CA repeats step 6 using the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st SO card **4** of 7<br>2nd SO card **3** of 7<br>3rd SO card **2** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:18 |

# Change the API Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 10 | CA performs the following steps to change the API settings:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"5.Key Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert CO Card #X?"** is displayed, insert the CO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the CO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd CO card.<br>g) Select **"5. API Settings"**, press **ENT** to confirm.<br>h) Select **"1.Key Import"**, press **ENT** to confirm.<br>i) When **"Key Import On Disable?"** is displayed, press **ENT** to confirm.<br>j) Select **"2.Key Export"**, press **ENT** to confirm.<br>k) When **"Key Export On Disable?"** is displayed, press **ENT** to confirm.<br>l) Select **"5.Sym Key Der"**, press **ENT** to confirm.<br>m) When **"Sym Key Der On Disable?"** is displayed, press **ENT** to confirm.<br>n) Press **CLR twice** to return to the main menu **"Secured"**.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st CO card **4** of 7<br>2nd CO card **3** of 7<br>3rd CO card **2** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 10:20 |

## Verify API Settings

| Step | Activity | Initials | Time |
|---|---|---|---|
| 11 | CA performs the following steps to dump the status of the HSM:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"4.HSM Info"**, press **ENT** to confirm.<br>c) Select **"8.Output Info"**, press **ENT** to confirm.<br>d) When **"Output Info?"** is displayed, press **ENT** to confirm.<br>e) Press **CLR** to return to the main menu **"Secured"**.<br><br>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:<br><br>`Modes: (1=Enabled 0=Disabled)`<br>`Global Key Export 1`<br>`App Key Import 0`<br>`App Key Export 0`<br>`Asymmetric Key Gen 1`<br>`Symmetric Key Gen 1`<br>`Symmetric Key Derive 0`<br>`Signing 1`<br>`Signature Verify 1`<br>`MAC Generation 1`<br>`MAC Verification 1`<br>`Encrypt / Decrypt 1`<br>`Delete Asym Key 1`<br>`Delete Sym Key 1`<br>`Output Key Details 1`<br>`Output Key Summary 1`<br>`Suite B Algorithms 1`<br>`Non Suite B Algs 1`<br>`Auto Online 0`<br>`Remote Management 0`<br>`AES SMK`<br>`Set Offline`<br>`FIPS Mode` | JD | 00:23 |

## App Key Backups

| Step | Activity | Initials | Time |
|---|---|---|---|
| 12 | CA performs the following steps to prepare the App key backups:<br>a) Remove the TEB from the cart and place it on the ceremony table.<br>b) Inspect the TEB for tamper evidence.<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used.<br>d) Remove and discard the TEB, then place the App key cards and the backup HSMFD on its designated area of the ceremony table.<br><br>**KSK-2017: TEB # BB91951258**<br>Last Verified: KSK Ceremony 44 2022-02-16<br><br>**Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.** | JD | 00:25 |

# Import the SMK and the KSK

| Step | Activity | Initials | Time |
|---|---|---|---|
| 13 | CA performs the following steps to access the Key Management menu:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"5.Key Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert CO Card #X?"** is displayed, insert the CO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the CO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd CO card.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st CO card **3** of 7<br>2nd CO card **2** of 7<br>3rd CO card **1** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:27 |
| 14 | CA performs the following steps to import the SMK:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm.<br>c) Select **"3.Restore SMK"**, press **ENT** to confirm.<br>d) When **"Restore SMK?"** is displayed, press **ENT** to confirm.<br>e) When **"Insert Card SMK #X?"** is displayed, insert the SMK card.<br>f) When **"Remove Card?"** is displayed, remove the SMK card.<br>g) Repeat steps e) to f) for the 2nd and 3rd SMK card.<br>h) When **"SMK Restored"** is displayed, press **ENT** to confirm.<br>i) Press **CLR** once to return to the main menu **"Key Mgmt"**.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **2**<br>1st SMK card **7** of 7<br>2nd SMK card **6** of 7<br>3rd SMK card **5** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:29 |
| 15 | CA performs the following steps to import KSK:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm.<br>c) Select **"2.Restore"**, press **ENT** to confirm.<br>d) When **"Restore?"** is displayed, press **ENT** to confirm.<br>e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm.<br>f) When **"Insert Card #X?"** is displayed, insert the required KSK card.<br>g) When **"Remove Card?"** is displayed, remove the KSK card.<br>h) When **"Restore Complete"** is displayed, press **ENT** to confirm.<br>i) Press **CLR twice** to return to the main menu **"Secured"**.<br><br>CA uses the card listed below. Card is returned to its designated card holder after use.<br>App Key card # **2**<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:31 |

## Return the KSK into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 16 | CA places the KSK and the backup HSMFD into its designated new TEB, then seals it. | JD | 00:32 |
| 17 | CA performs the following steps:<br>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number matches below.<br>c) Initial the TEB along with IW using a ballpoint pen.<br>d) Give IW the sealing strips for post-ceremony inventory.<br>e) Place the KSK TEB on the cart.<br><br>**KSK-2017: TEB # BB02638568** | JD | 00:33 |

## Enable/Activate the HSM (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 18 | CA performs the following steps to activate the HSM:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"1.Set Online"**, press **ENT** to confirm.<br>c) When **"Set Online?"** is displayed, press **ENT** to confirm.<br>d) When **"Insert Card OP #X?"** is displayed, insert the OP card.<br>e) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>f) When **"Remove Card?"** is displayed, remove the OP card.<br>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **ON.**<br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st OP card **4** of 7<br>2nd OP card **3** of 7<br>3rd OP card **2** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:35 |

## Check the Network Connectivity Between Laptop and HSM

| Step | Activity | Initials | Time |
|---|---|---|---|
| 19 | CA connects the HSM to the laptop using an ethernet cable in the LAN ports. | JD | 00:35 |
| 20 | CA performs the following steps to test the network connectivity between laptop and HSM:<br>a) Use the **Commands** terminal window<br>b) Test connectivity by executing:<br>`ping hsm`<br>c) Wait for responses, then exit by pressing:<br>`Ctrl + C` | JD | 00:36 |

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

1 February 2023

The SHA256 hash of the 2023 Q2 KSR file is:

**ksr-root-2023-q2-0.xml:**

5fd01e5ad586cd76544f7a6948c2b5dd7c51837f59e13e62bf0e76288ee982cb

The PGP wordlist for the hash above is:

**PGP Words:** eyetooth savagery berserk existence sterling letterhead spindle impetus eating document keyboard guitarist deadbolt repellent scorecard tambourine kiwi enchanting Mohawk integrate endow tolerance concert gadgetry slingshot Atlantic inverse cellulose orca ultimate miser revival

Attested on behalf of Verisign by:

Duane Wessels
Fellow
Naming Operations
Verisign, Inc.

## Insert KSRFD Copy

| Step | Activity | Initials | Time |
|---|---|---|---|
| 21 | CA plugs the FD labeled **"KSRFD_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.<br>**Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.** | JD | 00:36 |

## Execute the KSR Signer for KSR 2023 Q2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 22 | CA executes the command below in the terminal window to sign the KSR file:<br>`ksrsigner /media/KSRFD_COPY/KSK48/ksr-root-2023-q2-0.xml` | JD | 00:37 |
| 23 | When the KSR signer displays the prompt:<br>`Activate HSM prior to accepting in the affirmative!! (y/N):`<br>CA confirms that the HSM is online, then enters **"y"** to proceed. | JD | 00:37 |

## Verify the KSR Hash for KSR 2023 Q2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 24 | When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator. | JD | 00:38 |
| 25 | Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"** | JD | 00:38 |
| 26 | CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in:<br>`/media/KSRFD_COPY/KSK48/skr-root-2023-q2-0.xml` | JD | 00:38 |

## Print Copies of the KSR Signer log

| Step | Activity | Initials | Time |
|---|---|---|---|
| 27 | CA executes the commands below using the terminal window to print the KSR Signer log:<br>a) `lpadmin -p HP -o copies-default=X`<br>**Note: Replace "X" with the amount of copies needed for the participants.**<br>b) `printlog $(ls -tr ksrsigner-202302*.log \| tail -n 1)` | JD | 00:41 |
| 28 | IW attaches a copy of the required ksrsigner log to their script. | JD | 00:41 |

## Verify the SKR copy hash

| Step | Activity | Initials | Time |
|---|---|---|---|
| 29 | CA read the SHA256 hash in PGP wordlist format for the generated SKR and the ceremony participants match the hash with the previous SKR. | JD | 00:41 |

```
Starting: ksrsigner /media/KSRFD_COPY/KSK48/ksr-root-2023-q2-0.xml (at Thu Feb  2 00:37:11 2023 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  Ultra Electronics AEP Networks
    Model:           Keyper 9860-2
    Serial:          H2110017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-01-01T00:00:00 2023-01-22T00:00:00  18733,00951   20326(Klajeyz)/S
2  2023-01-11T00:00:00 2023-02-01T00:00:00  00951         20326(Klajeyz)/S
3  2023-01-21T00:00:00 2023-02-11T00:00:00  00951         20326(Klajeyz)/S
4  2023-01-31T00:00:00 2023-02-21T00:00:00  00951         20326(Klajeyz)/S
5  2023-02-10T00:00:00 2023-03-03T00:00:00  00951         20326(Klajeyz)/S
6  2023-02-20T00:00:00 2023-03-13T00:00:00  00951         20326(Klajeyz)/S
7  2023-03-02T00:00:00 2023-03-23T00:00:00  00951         20326(Klajeyz)/S
8  2023-03-12T00:00:00 2023-04-02T00:00:00  00951         20326(Klajeyz)/S
9  2023-03-22T00:00:00 2023-04-12T00:00:00  00951,60955   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSRFD_COPY/KSK48/ksr-root-2023-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  60955,00951
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955
...PASSED.

SHA256 hash of KSR:
5FD01E5AD586CD76544F7A6948C2B5DD7C51837F59E13E62BF0E76288EE982CB
>> eyetooth savagery berserk existence sterling letterhead spindle impetus eating document keyboard guitarist deadbolt re
pellent scorecard tambourine kiwi enchanting Mohawk integrate endow tolerance concert gadgetry slingshot Atlantic inverse
 cellulose orca ultimate miser revival <<

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSRFD_COPY/KSK48/skr-root-2023-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  00951,60955   20326(Klajeyz)/S
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955         20326(Klajeyz)/S
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955         20326(Klajeyz)/S
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955         20326(Klajeyz)/S
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955         20326(Klajeyz)/S
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955         20326(Klajeyz)/S
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955         20326(Klajeyz)/S
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955         20326(Klajeyz)/S
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955   20326(Klajeyz)/S

SHA256 hash of SKR:
13E107A29EEF9D818FC20CBDC8EFB1661CED9B280677B1C2308973C50BBB5CA9
>> Aztec tolerance ahead Pacific quiver unravel quadrant inventive payday repellent ammo quantity spaniel unravel sailboa
t gossamer befriend unify puppy cellulose afflict inception sailboat repellent chairlift matchmaker hockey resistor alone
 publisher escape passenger <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0
```

## Remove KSRFD copy

| Step | Activity | Initials | Time |
|---|---|---|---|
| 30 | CA executes the following commands using the terminal window:<br>a) List the contents of the KSRFD by executing:<br>`ls -ltrR /media/KSRFD_COPY`<br>b) Unmount the KSRFD by executing:<br>`umount /media/KSRFD_COPY` | JD | 00:42 |
| 31 | CA removes the **KSRFD_COPY** containing the SKR files, then gives it to IW for audit purpose. | JD | 00:42 |

## Disable/Deactivate the HSM (Tier 7)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 32 | CA deactivates the HSM by performing the following steps:<br>**Note: CA will use OP cards not previously utilized in this ceremony if available.**<br>a) CA displays the HSM activity logging terminal window<br>b) Utilize the HSM's keyboard to scroll through the menu using < ><br>c) Select **"2.Set Offline"**, press **ENT** to confirm.<br>d) When **"Set Offline?"** is displayed, press **ENT** to confirm.<br>e) When **"Insert Card OP #X?"** is displayed, insert the OP card from the card holder.<br>f) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>g) When **"Remove Card?"** is displayed, remove the OP card.<br>h) Repeat steps d) to f) for the 2nd and 3rd OP cards.<br><br>Confirm the **"READY"** LED on the **HSM** is **OFF.**<br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st OP card **3** of 7<br>2nd OP card **2** of 7<br>3rd OP card **1** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:44 |

# Root DNSSEC Script Exception

## Exception Details

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | IW writes the details of the ceremony exception:<br>Act: 5 Step(s): 36 Page(s): 34<br>Date and Time: 02-02-2023 00:52<br>**Note: IW describes the exception(s) and action(s) below.** | JD | 00:52 |

WHEN PLACING THE HSM INTO THE TEB, IT APPEARED TO HAVE SCRATCHED THE TEB. TO BE SAFE, IT WAS DECIDED TO REPLACE THE TEB. THE NEW TEB # BB51184520 / SERIAL # H2110017

THE OLD TEB # BB51184546 / SERIAL # H2110017

## Clear and Destroy AAK Cards

| Step | Activity | Initials | Time |
|---|---|---|---|
| 33 | CA performs the following steps to clear Adapter Authorization Key (AAK) cards:<br>a) Utilize the HSM's keyboard to scroll through the menu using < ><br>b) Select **"7.Role Mgmt"**, press **ENT** to confirm.<br>c) When **"Insert Card SO #X?"** is displayed, insert the SO card.<br>d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**.<br>e) When **"Remove Card?"** is displayed, remove the SO card.<br>f) Repeat steps c) to e) for the 2nd and 3rd SO card.<br>g) Select **"5.Clear AAK Card"**, press **ENT** to confirm.<br>h) When **"Clear AAK Card?"** is displayed, press **ENT** to confirm.<br>i) When **"Num Cards?"** is displayed, enter **"2"**, then press **ENT**.<br>j) When **"Insert Card AAK #X?"** is displayed, take the **AAK #X** card from the cardholder, show the **AAK #X** card to the audit camera and then insert the **AAK #X** card into the HSM's card reader.<br>k) When **"Are you sure?"** is displayed, press **ENT** to confirm.<br>l) When **"Remove Card?"** is displayed, remove the AAK card.<br>m) Repeat steps j) to l) for the 2nd AAK card.<br>n) Press **CLR** to return to the main menu **"Secured"**.<br><br>CA uses the cards listed below. Each card is returned to its designated card holder after use.<br>Set # **1**<br>1st SO card **3** of 7<br>2nd SO card **2** of 7<br>3rd SO card **1** of 7<br><br>**Note: If the card is unreadable, gently wipe its metal contacts and try again.** | JD | 00:47 |
| 34 | CA uses the shredder to destroy the cleared AAK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder. | JD | 00:49 |

## Place the HSM (Tier 7) into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 35 | CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.<br>**Note: DO NOT unplug the cable connections on the laptop.** | JD | 00:49 |
| 36 | CA places the HSM into its designated new TEB, then seals it. | JD | 00:56 |
| 37 | CA performs the following steps:<br>a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number and HSM serial number match below.<br>c) Initial the TEB along with IW using a ballpoint pen.<br>d) Give IW the sealing strips for post-ceremony inventory.<br>e) Place the HSM TEB on the cart.<br>BB61184520<br>**HSM7W: TEB # ~~BB51184546~~ / Serial # H2110017** | JD | 00:57 |

# 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' cards to Safe #2

## Stop Logging the Serial Output and the Terminal Session

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | CA performs the following steps to stop logging:<br>a) Disconnect the null modem and ethernet cables from the laptop.<br>b) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**:<br>i) Press `Ctrl + C`<br>ii) Execute `exit`<br>c) Execute the command below using the **Commands** terminal window to stop logging the terminal session:<br>`exit`<br>**Note: The Commands terminal session window will remain open.** | JD | 00:58 |

## Print Logging Information

| Step | Activity | Initials | Time |
|---|---|---|---|
| 2 | CA executes the following commands using the terminal window to print a copy of the logging information:<br>a) `lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true`<br>b) `enscript -2Gr script-202302*.log`<br>c) `enscript -Gr --font="Courier8" ttyaudit-tty*-202302*.log`<br><br>Attach the printed copies to IW script.<br>**Note: Ignore the error regarding non-printable characters if prompted.** | JD | 01:00 |

```
Script started on Wed Feb  1 22:02:34 2023
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=0.811 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.573 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.691 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.570 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.570/0.661/0.811/0.100 ms
root@coen:/media/HSMFD# ksrsigner /media/KSRFD/k\007\00KSK48/ks\007r-root-2023-q2-0.xml
Starting: ksrsigner /media/KSRFD/KSK48/ksr-root-2023-q2-0.xml (at Wed Feb  1 23:11:51 202
3 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:         H2008009

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-01-01T00:00:00 2023-01-22T00:00:00  18733,00951   20326(Klajeyz)/S
2  2023-01-11T00:00:00 2023-02-01T00:00:00  00951         20326(Klajeyz)/S
3  2023-01-21T00:00:00 2023-02-11T00:00:00  00951         20326(Klajeyz)/S
4  2023-01-31T00:00:00 2023-02-21T00:00:00  00951         20326(Klajeyz)/S
5  2023-02-10T00:00:00 2023-03-03T00:00:00  00951         20326(Klajeyz)/S
6  2023-02-20T00:00:00 2023-03-13T00:00:00  00951         20326(Klajeyz)/S
7  2023-03-02T00:00:00 2023-03-23T00:00:00  00951         20326(Klajeyz)/S
8  2023-03-12T00:00:00 2023-04-02T00:00:00  00951         20326(Klajeyz)/S
9  2023-03-22T00:00:00 2023-04-12T00:00:00  00951,60955   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSRFD/KSK48/ksr-root-2023-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  60955,00951
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955
...PASSED.

SHA256 hash of KSR:
5FD01E5AD586CD76544F7A6948C2B5DD7C51837F59E13E62BF0E76288EE982CB
>> eyetooth savagery berserk existence sterling letterhead spindle impetus eating documen
t keyboard guitarist deadbolt repellent scorecard tambourine kiwi enchanting Mohawk integ
rate endow tolerance concert gadgetry slingshot Atlantic inverse cellulose orca ultimate
miser revival <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSRFD/KSK48/skr-root-2023-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  00951,60955   20326(Klajeyz)/S
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955         20326(Klajeyz)/S
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955         20326(Klajeyz)/S
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955         20326(Klajeyz)/S
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955         20326(Klajeyz)/S
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955         20326(Klajeyz)/S
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955         20326(Klajeyz)/S
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955         20326(Klajeyz)/S
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955   20326(Klajeyz)/S

SHA256 hash of SKR:
13E107A29EEF9D818FC20CBDC8EFB1661CED9B280677B1C2308973C50BBB5CA9
>> Aztec tolerance ahead Pacific quiver unravel quadrant inventive payday repellent ammo
quantity spaniel unravel sailboat gossamer befriend unify puppy cellulose afflict incepti
on sailboat repellent chairlift matchmaker hockey resistor alone publisher escape passeng
er <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20230201-231151.log **********
root@coen:/media/HSMFD# lpadmin -p HP -o cppiea-default=12
root@coen:/media/HSMFD# p[illegible]\007\007\007\007\007\007\007lpadmin -p HP -o copies-defau
lt=12
root@coen:/media/HSMFD# ppadmin -p HP -o copies-default=13
root@coen:/media/HSMFD# prin\007tlog ks\007r\007signer\007-202302*.l\007og
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -l\007trR /media/KSRFD/
/media/KSRFD:
total 16
drwxr-xr-x 2 root root 16384 Feb  1 23:14 \033[0m\033[01;34mKSK48\033[0m

/media/KSRFD/KSK48:
total 144
-rw-r--r-- 1 root root 20369 Jan 20 18:01 skr.xml.20230201231151
-rw-r--r-- 1 root root 19596 Jan 20 18:01 ksr-root-2023-q2-0.xml
-rw-r--r-- 1 root root  1148 Jan 20 18:01 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb  1 23:14 skr.xml
-rw-r--r-- 1 root root 20369 Feb  1 23:14 skr-root-2023-q2-0.xml
root@coen:/media/HSMFD# cp -pR /media/KSRFD/KSK48/
root@coen:/media/HSMFD# l007pwd
/media/HSMFD
root@coen:/media/HSMFD# ls -ltrR
.:
total 3528
-rw-r--r-- 1 root root  15547 Jun  9  2010 ksr-root-2010-q3-2.xml
-rw-r--r-- 1 root root  40555 Jun  9  2010 wksr-20100517-172720.log
-rw-r--r-- 1 root root    190 Jun 16  2010 KSKSlotDB.config.db
-rw-r--r-- 1 root root   2668 Jun 16  2010 kskgen-20100616-211906.log
-rw-r--r-- 1 root root    765 Jun 16  2010 Kjqmt7v.csr
```

```
-rw-r--r-- 1 root root  36864 Jun 16  2010 ttyaudit-ttyUSB1-20100616-182157.log
-rw-r--r-- 1 root root  45056 Jun 16  2010 ttyaudit-ttyUSB0-20100616-182157.log
-rw-r--r-- 1 root root  18364 Jun 16  2010 skr-root-2010-q3-2.xml
-rw-r--r-- 1 root root   4473 Jun 16  2010 ksrsigner-20100616-214329.log
-rw-r--r-- 1 root root 196608 Jun 16  2010 script-20100616.log
-rw-r--r-- 1 root root   4096 Jun 16  2010 script-20100616-2209utc.log
-rw-r--r-- 1 root root  15547 Jul  8  2010 wksr_1_20100708144111_14165_198.41.3.50_ksr-ro
ot-2010-q4-1.xml
-rw-r--r-- 1 root root  30915 Jul  8  2010 wksr-20100708-144111.log
-rw-r--r-- 1 root root  15547 Jul  8  2010 ksr-root-2010-q4-1.xml
-rw-r--r-- 1 root root   1400 Jul 12  2010 ksrsigner-20100712-224252.log
-rw-r--r-- 1 root root  18364 Jul 12  2010 skr.xml.20100712224426
-rw-r--r-- 1 root root  18364 Jul 12  2010 skr-root-2010-q4-1.xml
-rw-r--r-- 1 root root   5506 Jul 12  2010 ksrsigner-20100712-224426.log
-rw-r--r-- 1 root root  36885 Jul 12  2010 ttyaudit-ttyUSB0-20100712-212549.log
-rw-r--r-- 1 root root  38221 Jul 12  2010 ttyaudit-ttyUSB1-20100712-212549.log
-rw-r--r-- 1 root root  12956 Jul 12  2010 script-20100712.log
-rw-r--r-- 1 root root  18402 Nov  1  2010 skr.xml.20110207223256
-rw-r--r-- 1 root root  15547 Jan  2  2011 ksr-root-2011-q2-0.xml
-rw-r--r-- 1 root root    188 Feb  7  2011 ksrsigner-20110207-223245.log
-rw-r--r-- 1 root root  18402 Feb  7  2011 skr-root-2011-q2-0.xml
-rw-r--r-- 1 root root   5524 Feb  7  2011 ksrsigner-20110207-223256.log
-rw-r--r-- 1 root root  13997 Feb  7  2011 ttyaudit-ttyUSB0-20110207-221818.log
-rw-r--r-- 1 root root  20709 Feb  7  2011 script-20110207.log
-rw-r--r-- 1 root root  18402 May 11  2011 skr.xml.20110720205839
-rw-r--r-- 1 root root  15551 Jul 19  2011 ksr-root-2011-q4-0.xml
-rw-r--r-- 1 root root  18404 Jul 20  2011 skr-root-2011-q4-0.xml
-rw-r--r-- 1 root root   5508 Jul 20  2011 ksrsigner-20110720-205839.log
-rw-r--r-- 1 root root   8044 Jul 20  2011 ttyaudit-ttyUSB0-20110720-205011.log
-rw-r--r-- 1 root root  32768 Jul 20  2011 script-20110720.log
-rw-r--r-- 1 root root  18422 Sep 30  2011 skr.xml.20120202222928
-rw-r--r-- 1 root root  15591 Jan  9  2012 ksr-root-2012-q2-0.xml
-rw-r--r-- 1 root root  18424 Feb  2  2012 skr-root-2012-q2-0.xml
-rw-r--r-- 1 root root   5509 Feb  2  2012 ksrsigner-20120202-222928.log
-rw-r--r-- 1 root root   8290 Feb  2  2012 ttyaudit-ttyUSB0-20120202-221813.log
-rw-r--r-- 1 root root  42056 Feb  2  2012 script-20120202.log
-rw-r--r-- 1 root root  18414 May 22  2012 skr.xml.20120726185458
-rw-r--r-- 1 root root  15391 Jul  3  2012 ksr-root-2012-q4-0.xml
-rw-r--r-- 1 root root  18324 Jul 26  2012 skr-root-2012-q4-0.xml
-rw-r--r-- 1 root root   5504 Jul 26  2012 ksrsigner-20120726-185458.log
-rw-r--r-- 1 root root  12034 Jul 26  2012 ttyaudit-ttyUSB0-20120726-184435.log
-rw-r--r-- 1 root root   5909 Jul 26  2012 script-20120726.log
-rw-r--r-- 1 root root  18314 Nov 12  2012 skr.xml.20130212222429
-rw-r--r-- 1 root root  15371 Jan 20  2013 ksr-root-2013-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 12  2013 skr-root-2013-q2-0.xml
-rw-r--r-- 1 root root   5506 Feb 12  2013 ksrsigner-20130212-222429.log
-rw-r--r-- 1 root root  12034 Feb 12  2013 ttyaudit-ttyUSB0-20130212-220521.log
-rw-r--r-- 1 root root   8385 Feb 12  2013 script-20130212.log
-rw-r--r-- 1 root root  18314 May  2  2013 skr.xml.20130807214313
-rw-r--r-- 1 root root  15371 Aug  5  2013 ksr-root-2013-q4-0.xml
-rw-r--r-- 1 root root  18314 Aug  7  2013 skr-root-2013-q4-0.xml
-rw-r--r-- 1 root root   5513 Aug  7  2013 ksrsigner-20130807-214313.log
-rw-r--r-- 1 root root   8192 Aug  7  2013 ttyaudit-ttyUSB0-20130807-213355.log
-rw-r--r-- 1 root root   5676 Aug  7  2013 script-20130807.log
-rw-r--r-- 1 root root  18314 Oct 24  2013 skr.xml.20140213225938
-rw-r--r-- 1 root root  15369 Jan 14  2014 ksr-root-2014-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 13  2014 skr-root-2014-q2-0.xml
-rw-r--r-- 1 root root   5513 Feb 13  2014 ksrsigner-20140213-225938.log
-rw-r--r-- 1 root root  12034 Feb 13  2014 ttyaudit-ttyUSB0-20140213-224635.log
-rw-r--r-- 1 root root   5638 Feb 13  2014 script-20140213.log
-rw-r--r-- 1 root root  18314 Apr 17  2014 skr.xml.20140814212827
-rw-r--r-- 1 root root  15369 Jul  7  2014 ksr-root-2014-q4-0.xml
-rw-r--r-- 1 root root      0 Aug 14  2014 ttyaudit-ttyUSB0-20140814-211101.log
-rw-r--r-- 1 root root  18314 Aug 14  2014 skr-root-2014-q4-0.xml
-rw-r--r-- 1 root root   5523 Aug 14  2014 ksrsigner-20140814-212827.log
-rw-r--r-- 1 root root  12032 Aug 14  2014 ttyaudit-ttyUSB0-20140814-211416.log
-rw-r--r-- 1 root root   5563 Aug 14  2014 script-20140814.log
-rw-r--r-- 1 root root  18314 Nov 20  2014 skr.xml.20150122223324
-rw-r--r-- 1 root root  15369 Jan 13  2015 ksr-root-2015-q2-0.xml
-rw-r--r-- 1 root root    762 Jan 13  2015 hash_ksr20.txt
-rw-r--r-- 1 root root  18314 Jan 22  2015 skr-root-2015-q2-0.xml
-rw-r--r-- 1 root root   5526 Jan 22  2015 ksrsigner-20150122-223324.log
-rw-r--r-- 1 root root  12034 Jan 22  2015 ttyaudit-ttyUSB0-20150122-222401.log
-rw-r--r-- 1 root root   5941 Jan 22  2015 script-20150122.log
-rw-r--r-- 1 root root  18314 Jul 28  2015 skr.xml.20150813213057
-rw-r--r-- 1 root root  15369 Jul 28  2015 ksr-root-2015-q4-0.xml
-rw-r--r-- 1 root root  18314 Aug 13  2015 skr-root-2015-q4-0.xml
-rw-r--r-- 1 root root   5505 Aug 13  2015 ksrsigner-20150813-213057.log
-rw-r--r-- 1 root root  17517 Aug 13  2015 ttyaudit-ttyUSB0-20150813-211033.log
-rw-r--r-- 1 root root   5520 Aug 13  2015 ksrsigner-20150814-000517.log
-rw-r--r-- 1 root root  43054 Aug 13  2015 ttyaudit-ttyUSB0-20150813-220137.log
-rw-r--r-- 1 root root   5520 Aug 13  2015 ksrsigner-20150814-002123.log
-rw-r--r-- 1 root root  44497 Aug 13  2015 ttyaudit-ttyUSB1-20150813-220137.log
-rw-r--r-- 1 root root  28755 Aug 13  2015 script-20150813.log
-rw-r--r-- 1 root root  18314 Jan 14  2016 skr.xml.20160211235227
-rw-r--r-- 1 root root  15371 Jan 14  2016 ksr-root-2016-q2-0.xml
-rw-r--r-- 1 root root  18314 Feb 11  2016 skr-root-2016-q2-0.xml
-rw-r--r-- 1 root root   5530 Feb 11  2016 ksrsigner-20160211-235227.log
-rw-r--r-- 1 root root  12196 Feb 11  2016 ttyaudit-ttyUSB0-20160211-234001.log
-rw-r--r-- 1 root root   6919 Feb 11  2016 script-20160211.log
-rw-r--r-- 1 root root  17908 May 12  2016 skr.xml.20160811220932
-rw-r--r-- 1 root root  14301 Jul 13  2016 ksr-root-2016-q4-fallback-1.xml
-rw-r--r-- 1 root root  21718 Jul 13  2016 ksr-root-2016-q4-0.xml
-rw-r--r-- 1 root root  18599 Jul 20  2016 skr.xml.20160811215735
-rw-r--r-- 1 root root  21083 Aug 11  2016 skr-root-2016-q4-0.xml
-rw-r--r-- 1 root root   5520 Aug 11  2016 ksrsigner-20160811-215735.log
-rw-r--r-- 1 root root  17908 Aug 11  2016 skr-root-2016-q4-fallback-1.xml
-rw-r--r-- 1 root root   5694 Aug 11  2016 ksrsigner-20160811-220932.log
-rw-r--r-- 1 root root  12499 Aug 11  2016 ttyaudit-ttyUSB0-20160811-213430.log
-rw-r--r-- 1 root root  33540 Aug 11  2016 ttyaudit-ttyUSB0-20160811-222510.log
-rw-r--r-- 1 root root  21200 Aug 11  2016 script-20160811.log
-rw-r--r-- 1 root root  20348 Oct 27  2016 skr.xml.20170202225202
-rw-r--r-- 1 root root  19556 Jan  4  2017 ksr-root-2017-q2-0.xml
-rw-r--r-- 1 root root  20347 Feb  2  2017 skr.xml
-rw-r--r-- 1 root root  20347 Feb  2  2017 skr-root-2017-q2-0.xml
-rw-r--r-- 1 root root   5494 Feb  2  2017 ksrsigner-20170202-225202.log
-rw-r--r-- 1 root root    357 Feb  2  2017 keybackup-20170203-001846.log
-rw-r--r-- 1 root root   2693 Feb  2  2017 kskgen-20170203-001954.log
-rw-r--r-- 1 root root    817 Feb  2  2017 Klajeyz.csr
-rw-r--r-- 1 root root    357 Feb  2  2017 keybackup-20170203-003825.log
-rw-r--r-- 1 root root  48066 Feb  2  2017 ttyaudit-ttyUSB0-20170202-223524.log
-rw-r--r-- 1 root root  23999 Feb  2  2017 script-20170202.log
-rw-r--r-- 1 root root      0 Aug 17  2017 script-20170817.log
-rw-r--r-- 1 root root   8192 Aug 17  2017 ttyaudit-ttyUSB0-20170817-211909.log
-rw-r--r-- 1 root root   6645 Aug 17  2017 ksrsigner-20170817-214009.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[0m\033[01;34mKSK30-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6648 Aug 17  2017 ksrsigner-20170817-214402.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6662 Aug 17  2017 ksrsigner-20170817-214602.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6355 Aug 17  2017 ksrsigner-20170817-214756.log
drwxr-xr-x 2 root root   8192 Aug 17  2017 \033[01;34mKSK30-3-C_to_C\033[0m
-rw-r--r-- 1 root root   2484 Aug 17  2017 ttyaudit-ttyUSB0-20170817-213501.log
-rw-r--r-- 1 root root  65904 Aug 17  2017 script-20170817-2.log
-rw-r--r-- 1 root root   6689 Feb  7  2018 ksrsigner-20180207-224219.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6676 Feb  7  2018 ksrsigner-20180207-224724.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-1-E_to_D\033[0m
```

```
-rw-r--r-- 1 root root   6674 Feb  7  2018 ksrsigner-20180207-224920.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6367 Feb  7  2018 ksrsigner-20180207-225053.log
drwxr-xr-x 2 root root   8192 Feb  7  2018 \033[01;34mKSK32-3-C_to_C\033[0m
-rw-r--r-- 1 root root  13737 Feb  7  2018 ttyaudit-ttyUSB0-20180207-222555.log
-rw-r--r-- 1 root root  23281 Feb  7  2018 script-20180207.log
-rw-r--r-- 1 root root   6774 Aug 15  2018 ksrsigner-20180815-221523.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-0-D_to_E\033[0m
-rw-r--r-- 1 root root   6788 Aug 15  2018 ksrsigner-20180815-221858.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-1-E_to_D\033[0m
-rw-r--r-- 1 root root   6798 Aug 15  2018 ksrsigner-20180815-222046.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-2-D_to_D\033[0m
-rw-r--r-- 1 root root   6453 Aug 15  2018 ksrsigner-20180815-222210.log
drwxr-xr-x 2 root root   8192 Aug 15  2018 \033[01;34mKSK34-3-C_to_C\033[0m
-rw-r--r-- 1 root root  14348 Aug 15  2018 ttyaudit-ttyS0-20180815-220248.log
-rw-r--r-- 1 root root  24749 Aug 15  2018 script-20180815.log
-rw-r--r-- 1 root root   6420 Feb 27  2019 ksrsigner-20190227-222718.log
drwxr-xr-x 2 root root   8192 Feb 27  2019 \033[01;34mKSK36\033[0m
-rw-r--r-- 1 root root  12372 Feb 27  2019 ttyaudit-ttyS0-20190227-221242.log
-rw-r--r-- 1 root root  22453 Feb 27  2019 script-20190227.log
-rw-r--r-- 1 root root   6252 Aug 14  2019 ksrsigner-20190814-215719.log
drwxr-xr-x 2 root root   8192 Aug 14  2019 \033[01;34mKSK38\033[0m
-rw-r--r-- 1 root root    357 Aug 14  2019 keybackup-20190814-231635.log
-rw-r--r-- 1 root root    210 Aug 14  2019 keybackup-20190814-231754.log
-rw-r--r-- 1 root root   1493 Aug 14  2019 KSKSlotDB.db
-rw-r--r-- 1 root root    271 Aug 14  2019 keybackup-20190814-231804.log
-rw-r--r-- 1 root root   6267 Aug 15  2019 ksrsigner-20190815-002322.log
-rw-r--r-- 1 root root  89867 Aug 15  2019 ttyaudit-ttyS0-20190814-213756.log
-rw-r--r-- 1 root root  29833 Aug 15  2019 script-20190814.log
-rw-r--r-- 1 root root   6280 Feb 16  2020 ksrsigner-20200216-022133.log
drwxr-xr-x 2 root root   8192 Feb 16  2020 \033[01;34mKSK40\033[0m
-rw-r--r-- 1 root root  12174 Feb 16  2020 ttyaudit-ttyS0-20200216-020929.log
-rw-r--r-- 1 root root  23671 Feb 16  2020 script-20200216.log
-rw-r--r-- 1 root root   6308 Apr 23  2020 ksrsigner-20200423-184208.log
drwxr-xr-x 2 root root   8192 Apr 23  2020 \033[01;34mKSK41-2020-Q3\033[0m
-rw-r--r-- 1 root root   7151 Apr 23  2020 ksrsigner-20200423-185053.log
drwxr-xr-x 2 root root   8192 Apr 23  2020 \033[01;34mKSK41-2020-Q4\033[0m
-rw-r--r-- 1 root root   7151 Apr 23  2020 ksrsigner-20200423-185433.log
drwxr-xr-x 2 root root   8192 Apr 23  2020 \033[01;34mKSK41-2021-Q1\033[0m
-rw-r--r-- 1 root root  15125 Apr 23  2020 ttyaudit-ttyS0-20200423-182706.log
-rw-r--r-- 1 root root  36962 Apr 23  2020 script-20200423.log
-rw-r--r-- 1 root root   6295 Feb 11  2021 ksrsigner-20210211-191856.log
drwxr-xr-x 2 root root   8192 Feb 11  2021 \033[01;34mKSK42-2021-Q2\033[0m
-rw-r--r-- 1 root root   6958 Feb 11  2021 ksrsigner-20210211-192546.log
drwxr-xr-x 2 root root   8192 Feb 11  2021 \033[01;34mKSK42-2021-Q3\033[0m
-rw-r--r-- 1 root root   7169 Feb 11  2021 ksrsigner-20210211-192952.log
drwxr-xr-x 2 root root   8192 Feb 11  2021 \033[01;34mKSK42-2021-Q4\033[0m
-rw-r--r-- 1 root root  13763 Feb 11  2021 ttyaudit-ttyS0-20210211-190608.log
-rw-r--r-- 1 root root  38580 Feb 11  2021 script-20210211.log
-rw-r--r-- 1 root root   6248 Feb 16  2022 ksrsigner-20220216-224254.log
drwxr-xr-x 2 root root   8192 Feb 16  2022 \033[01;34mKSK44\033[0m
-rw-r--r-- 1 root root   6263 Feb 16  2022 ksrsigner-20220216-234715.log
-rw-r--r-- 1 root root  65325 Feb 17  2022 ttyaudit-ttyS0-20220216-222905.log
-rw-r--r-- 1 root root  34299 Feb 17  2022 script-20220216.log
drwxr-xr-x 2 root root   8192 Aug 17 21:22 \033[01;34mKSK46\033[0m
-rw-r--r-- 1 root root   6251 Aug 17 21:22 ksrsigner-20220817-211649.log
-rw-r--r-- 1 root root  85626 Aug 17 22:38 ttyaudit-ttyS0-20220817-205940.log
-rw-r--r-- 1 root root  28220 Aug 17 22:56 script-20220817.log
-rw-r--r-- 1 root root      0 Feb  1 22:02 script-20230201.log
-rw-r--r-- 1 root root  21867 Feb  1 23:14 ttyaudit-ttyS0-20230201-220329.log
drwxr-xr-x 2 root root   8192 Feb  1 23:14 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root   6262 Feb  1 23:14 ksrsigner-20230201-231151.log
drwxr-xr-x 2 root root   8192 Feb  1 23:14 \033[01;34mKSK48\033[0m
```

```
./KSK30-0-D_to_E:
total 120
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214009
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr-root-2017-q4-0-d_to_e.xml

./KSK30-1-E_to_D:
total 120
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214402
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr-root-2017-q4-1-e_to_d.xml

./KSK30-2-D_to_D:
total 120
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214602
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 24928 Aug 17  2017 skr-root-2017-q4-2-d_to_d.xml

./KSK30-3-C_to_C:
total 104
-rw-r--r-- 1 root root 24419 Aug 15  2017 skr.xml.20170817214756
-rw-r--r-- 1 root root 19556 Aug 15  2017 ksr-root-2017-q4-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Aug 15  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Aug 17  2017 skr.xml
-rw-r--r-- 1 root root 20347 Aug 17  2017 skr-root-2017-q4-3-c_to_c.xml

./KSK32-0-D_to_E:
total 128
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207224219
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr-root-2018-q2-0-d_to_e.xml

./KSK32-1-E_to_D:
total 128
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207224724
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr-root-2018-q2-1-e_to_d.xml

./KSK32-2-D_to_D:
total 128
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207224920
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 24928 Feb  7  2018 skr-root-2018-q2-2-d_to_d.xml

./KSK32-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Jan 29  2018 skr.xml.20180207225053
-rw-r--r-- 1 root root 19556 Jan 29  2018 ksr-root-2018-q2-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Jan 29  2018 kskschedule.json
-rw-r--r-- 1 root root 20347 Feb  7  2018 skr.xml
-rw-r--r-- 1 root root 20347 Feb  7  2018 skr-root-2018-q2-3-c_to_c.xml
```

```
./KSK34-0-D_to_E:
total 128
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815221523
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr-root-2018-q4-0-d_to_e.xml

./KSK34-1-E_to_D:
total 128
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815221858
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-1-e_to_d.xml
-rw-r--r-- 1 root root  1344 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr-root-2018-q4-1-e_to_d.xml

./KSK34-2-D_to_D:
total 128
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815222046
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-2-d_to_d.xml
-rw-r--r-- 1 root root  1344 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 24930 Aug 15  2018 skr-root-2018-q4-2-d_to_d.xml

./KSK34-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Aug  8  2018 skr.xml.20180815222210
-rw-r--r-- 1 root root 19542 Aug  8  2018 ksr-root-2018-q4-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Aug  8  2018 kskschedule.json
-rw-r--r-- 1 root root 20349 Aug 15  2018 skr.xml
-rw-r--r-- 1 root root 20349 Aug 15  2018 skr-root-2018-q4-3-c_to_c.xml

./KSK36:
total 112
-rw-r--r-- 1 root root 29640 Feb 20  2019 skr.xml.20190227222718
-rw-r--r-- 1 root root 19600 Feb 20  2019 ksr-root-2019-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb 20  2019 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 27  2019 skr.xml
-rw-r--r-- 1 root root 20369 Feb 27  2019 skr-root-2019-q2-0.xml

./KSK38:
total 104
-rw-r--r-- 1 root root 20369 Aug  6  2019 skr.xml.20190814215719
-rw-r--r-- 1 root root 19600 Aug  6  2019 ksr-root-2019-q4-0.xml
-rw-r--r-- 1 root root  1148 Aug  6  2019 kskschedule.json
-rw-r--r-- 1 root root 20369 Aug 14  2019 skr.xml
-rw-r--r-- 1 root root 20369 Aug 14  2019 skr-root-2019-q4-0.xml

./KSK40:
total 104
-rw-r--r-- 1 root root 20369 Feb  4  2020 skr.xml.20200216022133
-rw-r--r-- 1 root root 19600 Feb  4  2020 ksr-root-2020-q2-0.xml
-rw-r--r-- 1 root root  1148 Feb  4  2020 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16  2020 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16  2020 skr-root-2020-q2-0.xml

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

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

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

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

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

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

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

./KSK46:
total 104
-rw-r--r-- 1 root root 20369 Jul 11  2018 skr.xml.20220817211649
-rw-r--r-- 1 root root 19596 Jul 11  2018 ksr-root-2022-q4-0.xml
-rw-r--r-- 1 root root  1148 Jul 11  2018 kskschedule.json
-rw-r--r-- 1 root root 20369 Aug 17 21:22 skr.xml
-rw-r--r-- 1 root root 20369 Aug 17 21:22 skr-root-2022-q4-0.xml

./tmp:
total 72
-rw-r--r-- 1 root root 1768 Feb  1 23:14 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.3
```

```
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Feb  1 23:14 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Feb  1 23:14 skr.keybundle.0

./KSK48:
total 104
-rw-r--r-- 1 root root 20369 Jan 20 18:01 skr.xml.20230201231151
-rw-r--r-- 1 root root 19596 Jan 20 18:01 ksr-root-2023-q2-0.xml
-rw-r--r-- 1 root root  1148 Jan 20 18:01 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb  1 23:14 skr.xml
-rw-r--r-- 1 root root 20369 Feb  1 23:14 skr-root-2023-q2-0.xml
root@coen:/media/HSMFD# sh\007a2\007wordlist < KS\007K48/sk\007r-root-2023-q2-0.xml
SHA-256:    13e107a29eef9d818fc20cbdc8efb1661ced9b280677b1c2308973c50bbb5ca9
PGP Words:  Aztec tolerance ahead Pacific quiver unravel quadrant inventive payday repell
ent ammo quantity spaniel unravel sailboat gossamer befriend unify puppy cellulose afflic
t inception sailboat repellent chairlift matchmaker hockey resistor alone publisher escap
e passenger
root@coen:/media/HSMFD# umoun\007t /media/KSRFD/
root@coen:/media/HSMFD# [redacted]10.xml
PING hsm (192.168.0.2) 56(84) bytes of data.
64 bytes from hsm (192.168.0.2): icmp_seq=9 ttl=255 time=1.18 ms
64 bytes from hsm (192.168.0.2): icmp_seq=10 ttl=255 time=0.475 ms
64 bytes from hsm (192.168.0.2): icmp_seq=11 ttl=255 time=0.696 ms
64 bytes from hsm (192.168.0.2): icmp_seq=12 ttl=255 time=0.570 ms
64 bytes from hsm (192.168.0.2): icmp_seq=13 ttl=255 time=0.569 ms
^C
--- hsm ping statistics ---
13 packets transmitted, 5 received, 61% packet loss, time 12256ms
rtt min/avg/max/mdev = 0.475/0.699/1.185/0.252 ms
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=0.401 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.579 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.573 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.572 ms
64 bytes from hsm (192.168.0.2): icmp_seq=5 ttl=255 time=0.581 ms
^C
--- hsm ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4100ms
rtt min/avg/max/mdev = 0.401/0.541/0.581/0.071 ms
root@coen:/media/HSMFD# ksrsigner /media/KSRFD_COPY/KSK48/ks\007r-root-2023-q2-0.xml
Starting: ksrsigner /media/KSRFD_COPY/KSK48/ksr-root-2023-q2-0.xml (at Thu Feb  2 00:37:1
1 2023 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_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:          H2110017

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-01-01T00:00:00 2023-01-22T00:00:00  18733,00951   20326(Klajeyz)/S
2  2023-01-11T00:00:00 2023-02-01T00:00:00  00951         20326(Klajeyz)/S
3  2023-01-21T00:00:00 2023-02-11T00:00:00  00951         20326(Klajeyz)/S
4  2023-01-31T00:00:00 2023-02-21T00:00:00  00951         20326(Klajeyz)/S
5  2023-02-10T00:00:00 2023-03-03T00:00:00  00951         20326(Klajeyz)/S
6  2023-02-20T00:00:00 2023-03-13T00:00:00  00951         20326(Klajeyz)/S
7  2023-03-02T00:00:00 2023-03-23T00:00:00  00951         20326(Klajeyz)/S
8  2023-03-12T00:00:00 2023-04-02T00:00:00  00951         20326(Klajeyz)/S
9  2023-03-22T00:00:00 2023-04-12T00:00:00  00951,60955   20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSRFD_COPY/KSK48/ksr-root-2023-q2-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  60955,00951
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955
...PASSED.

SHA256 hash of KSR:
5FD01E5AD586CD76544F7A6948C2B5DD7C51837F59E13E62BF0E76288EE982CB
>> eyetooth savagery berserk existence sterling letterhead spindle impetus eating documen
t keyboard guitarist deadbolt repellent scorecard tambourine kiwi enchanting Mohawk integ
rate endow tolerance concert gadgetry slingshot Atlantic inverse cellulose orca ultimate
miser revival <<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
#  KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSRFD_COPY/KSK48/skr-root-2023-q2-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2023-04-01T00:00:00 2023-04-22T00:00:00  00951,60955   20326(Klajeyz)/S
2  2023-04-11T00:00:00 2023-05-02T00:00:00  60955         20326(Klajeyz)/S
3  2023-04-21T00:00:00 2023-05-12T00:00:00  60955         20326(Klajeyz)/S
4  2023-05-01T00:00:00 2023-05-22T00:00:00  60955         20326(Klajeyz)/S
5  2023-05-11T00:00:00 2023-06-01T00:00:00  60955         20326(Klajeyz)/S
6  2023-05-21T00:00:00 2023-06-11T00:00:00  60955         20326(Klajeyz)/S
7  2023-05-31T00:00:00 2023-06-21T00:00:00  60955         20326(Klajeyz)/S
8  2023-06-10T00:00:00 2023-07-01T00:00:00  60955         20326(Klajeyz)/S
9  2023-06-20T00:00:00 2023-07-11T00:00:00  11019,60955   20326(Klajeyz)/S

SHA256 hash of SKR:
13E107A29EEF9D818FC20CBDC8EFB1661CED9B280677B1C2308973C50BBB5CA9
>> Aztec tolerance ahead Pacific quiver unravel quadrant inventive payday repellent ammo
quantity spaniel unravel sailboat gossamer befriend unify puppy cellulose afflict incepti
on sailboat repellent chairlift matchmaker hockey resistor alone publisher escape passeng
er <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

********** Log output in ./ksrsigner-20230202-003711.log **********
root@coen:/media/HSMFD# lpadmin pp HP -o copies-default=12
```

```
root@coen:/media/HSMFD# [illegible]printlog $(ls -tr ks\007r\007s\007igner-203\002\0073\0070
20.log | tail -n 1)
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /media/KSRFD_COPY/
/media/KSRFD_COPY:
total 16
drwxr-xr-x 2 root root 16384 Feb  2 00:38 \033[0m\033[01;34mKSK48\033[0m

/media/KSRFD_COPY/KSK48:
total 144
-rw-r--r-- 1 root root 20369 Jan 20 18:15 skr.xml.20230202003711
-rw-r--r-- 1 root root 19596 Jan 20 18:15 ksr-root-2023-q2-0.xml
-rw-r--r-- 1 root root  1148 Jan 20 18:15 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb  2 00:38 skr.xml
-rw-r--r-- 1 root root 20369 Feb  2 00:38 skr-root-2023-q2-0.xml
root@coen:/media/HSMFD# umount /media/ks\007r\007SRFD_COPY/
k033[Kroot@media/HSMFD#HSMFD# exit
exit

Script done on Thu Feb  2 00:58:20 2023
```

```
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0   H2008009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0   BBL CRC32: 0xDBC9B9F2
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0   Running applicationBootLoader at 0xEFDC0000
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0   H2008009 011403 ABL 030 : Tamper Challenge Response Key
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:25+0000        ttyS0   ABL CRC32: 0xE7E0FA6A
2023-02-01T22:04:25+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   ####################################
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   ###     ABL tamper records       ###
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   ####################################
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   ====================================
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   vextoosTamperCount:     0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   vintoosTamperCount:     4
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   vbboosTamperCount:      0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   maxstrtempTamperCount:  0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   minstrtempTamperCount:  0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   meshTamperCount:        0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   extampSMKTamperCount:   0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   extampIMKTamperCount:   0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   tempdiffTamperCount:    0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   pfTamperCount:          4
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   restartTamperCount:     12
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   Current tamper bitmaps:
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   ======================
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   lastTamper bitmap:      0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
```

```
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   Bitmapped Change Record (most recent first):
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0   ========================================
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:26+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0   Running cryptoApplication at 0xEBF00000
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0   Jumping to startup @ 0x001037B4
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0   Board is P2020RDB
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0   board_smp_init: 2 cpu
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:27+0000        ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-02-01T22:04:27+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0   Starting next program at v0015183c
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0   Starting K-Series Kernel
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0   Copyright Ultra Electronics AEP. All Rights Reserved.
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:28+0000        ttyS0   Sat May  1 13:08:08 1971
2023-02-01T22:04:28+0000        ttyS0
2023-02-01T22:04:29+0000        ttyS0   Starting auditd v2.0 ... started.
2023-02-01T22:04:29+0000        ttyS0
2023-02-01T22:04:29+0000        ttyS0   Interface 0 configured for IPv6.
2023-02-01T22:04:29+0000        ttyS0
2023-02-01T22:04:29+0000        ttyS0   Interface 0 configured for IPv4.
2023-02-01T22:04:29+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   Interface 1 configured for IPv6.
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   Interface 1 configured for IPv4.
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   route: writing to routing socket: Network is unreachable
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   add net default: gateway ::: Network is unreachable
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   route: writing to routing socket: Network is unreachable
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   Starting USB driver...
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0   9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0
2023-02-01T22:04:30+0000        ttyS0
```

```
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running DES POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  DES POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running Triple DES POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Triple DES POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running AES POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  AES POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running SHA1 POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  SHA1 POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running SHA2 POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  SHA2 POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running RandomGen POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  RandomGen POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running RSA POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  RSA POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running DSA POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  DSA POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running SEED POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  SEED POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running RIPEMD160 POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  RIPEMD160 POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running ECC POST Test
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  ECC POST Test Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Running HMAC POST Tests
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  HMAC POST Tests Passed
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0  Audit on 1/5/1971 13:08:11 00100008
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0
2023-02-01T22:04:32+0000 ttyS0
```

```
2023-02-01T22:04:32+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Keyper 9860-2  Serial Number H2008009
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Memory Usage:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   RAM (free/total)         192Mb/256Mb
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Flash (free/total)       128Mb/128Mb
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0      black store           524b
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0      statistics            112b
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0      other                 116b
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   RedStore (free/total)    107Kb/128Kb
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Network Configuration:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Interface 0:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0       IPv4: enabled
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0       IPv6: enabled
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C8:52 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c852/64
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Interface 1:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0       IPv4: enabled
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0       IPv6: enabled
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0       MAC/IP address(es): 00:E0:6C:00:C8:53 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c853/64
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   HSM Port 0: 05000
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   HSM Port 1: 03000
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Default Gateway(s): 0.0.0.0 ::
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Software Versions:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   BBL 030 ABL 021 App 034
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   CPLD Version:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   1.9
2023-02-01T22:04:33+0000        ttyS0
```

```
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   SCR Firmware Version:
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   OROS-R2.99-R1.20
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   HmcListener: Created IPv4 socket 12 on port 3000.
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   HmcListener: Created IPv6 socket 13 on port 3000.
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:04:33+0000        ttyS0   Audit on 1/5/1971 13:08:12 00100003
2023-02-01T22:04:33+0000        ttyS0
2023-02-01T22:11:21+0000        ttyS0   Audit on 1/5/1971 13:15:00 00200023 0A400000DB46296E
2023-02-01T22:11:21+0000        ttyS0
2023-02-01T22:11:49+0000        ttyS0   Audit on 1/5/1971 13:15:27 00200023 0A400000B6C6296E
2023-02-01T22:11:49+0000        ttyS0
2023-02-01T22:12:32+0000        ttyS0   Audit on 1/5/1971 13:16:11 00200023 0A400000BA86296E
2023-02-01T22:12:32+0000        ttyS0
2023-02-01T22:13:59+0000        ttyS0   Audit on 1/5/1971 13:17:38 0020002f 398001161DA72A76
2023-02-01T22:13:59+0000        ttyS0
2023-02-01T22:14:52+0000        ttyS0   Audit on 1/5/1971 13:18:31 0020002f 398001161EA72A76
2023-02-01T22:14:52+0000        ttyS0
2023-02-01T22:16:13+0000        ttyS0   Audit on 1/5/1971 13:19:52 0020002f 39800115FA272A76
2023-02-01T22:16:13+0000        ttyS0
2023-02-01T22:16:54+0000        ttyS0   Audit on 1/5/1971 13:20:33 0020002f 3980011620E72A76
2023-02-01T22:16:54+0000        ttyS0
2023-02-01T22:17:33+0000        ttyS0   Audit on 1/5/1971 13:21:12 0020002f 398001161FE72A76
2023-02-01T22:17:33+0000        ttyS0
2023-02-01T22:18:26+0000        ttyS0   Audit on 1/5/1971 13:22:06 0020002f 398001160E272A76
2023-02-01T22:18:26+0000        ttyS0
2023-02-01T22:19:11+0000        ttyS0   Audit on 1/5/1971 13:22:50 0020002f 39800115FDA72A76
2023-02-01T22:19:11+0000        ttyS0
2023-02-01T22:19:22+0000        ttyS0   Audit on 1/5/1971 13:23:01 00200077 39800115FDA72A76
2023-02-01T22:19:22+0000        ttyS0
2023-02-01T22:20:26+0000        ttyS0   Audit on 1/5/1971 13:24:05 0020002f 398001161E272A76
2023-02-01T22:20:26+0000        ttyS0
2023-02-01T22:21:07+0000        ttyS0   Audit on 1/5/1971 13:24:46 0020002f 39800115F9E72A76
2023-02-01T22:21:07+0000        ttyS0
2023-02-01T22:21:49+0000        ttyS0   Audit on 1/5/1971 13:25:28 0020002f 39800115FAE72A76
2023-02-01T22:21:49+0000        ttyS0
2023-02-01T22:22:35+0000        ttyS0   Audit on 1/5/1971 13:26:14 0020002f 3980011620672A76
2023-02-01T22:22:35+0000        ttyS0
2023-02-01T22:23:17+0000        ttyS0   Audit on 1/5/1971 13:26:56 0020002f 3980011654672A76
2023-02-01T22:23:17+0000        ttyS0
2023-02-01T22:24:01+0000        ttyS0   Audit on 1/5/1971 13:27:40 0020002f 3980011604A72A76
2023-02-01T22:24:01+0000        ttyS0
2023-02-01T22:24:41+0000        ttyS0   Audit on 1/5/1971 13:28:19 0020002f 39800115FD272A76
2023-02-01T22:24:41+0000        ttyS0
2023-02-01T22:24:52+0000        ttyS0   Audit on 1/5/1971 13:28:31 00200077 39800115FD272A76
2023-02-01T22:24:52+0000        ttyS0
2023-02-01T22:26:15+0000        ttyS0   Audit on 1/5/1971 13:29:54 0020002f 3F400032D64A2A77
```

```
2023-02-01T22:26:15+0000 ttyS0
2023-02-01T22:27:02+0000 ttyS0   Audit on 1/5/1971 13:30:41 0020002f 3F400032D70A2A77
2023-02-01T22:27:02+0000 ttyS0
2023-02-01T22:27:41+0000 ttyS0   Audit on 1/5/1971 13:31:20 0020002f 3F400031D48A2A77
2023-02-01T22:27:41+0000 ttyS0
2023-02-01T22:28:22+0000 ttyS0   Audit on 1/5/1971 13:32:01 0020002f 3980011692A72A76
2023-02-01T22:28:22+0000 ttyS0
2023-02-01T22:29:15+0000 ttyS0   Audit on 1/5/1971 13:32:54 0020002f 3F4000339FCA2A77
2023-02-01T22:29:15+0000 ttyS0
2023-02-01T22:29:56+0000 ttyS0   Audit on 1/5/1971 13:33:35 0020002f 3F4000339F4A2A77
2023-02-01T22:29:56+0000 ttyS0
2023-02-01T22:30:35+0000 ttyS0   Audit on 1/5/1971 13:34:14 0020002f 3F4000339ECA2A77
2023-02-01T22:30:35+0000 ttyS0
2023-02-01T22:30:47+0000 ttyS0   Audit on 1/5/1971 13:34:26 00200063 3F4000339ECA2A77
2023-02-01T22:30:47+0000 ttyS0
2023-02-01T22:31:31+0000 ttyS0   Audit on 1/5/1971 13:35:10 0020002f 3F400032D68A2A77
2023-02-01T22:31:31+0000 ttyS0
2023-02-01T22:32:08+0000 ttyS0   Audit on 1/5/1971 13:35:47 0020002f 3F400033F88A2A77
2023-02-01T22:32:08+0000 ttyS0
2023-02-01T22:32:47+0000 ttyS0   Audit on 1/5/1971 13:36:26 0020002f 4780000181AD2972
2023-02-01T22:32:47+0000 ttyS0
2023-02-01T22:33:30+0000 ttyS0   Audit on 1/5/1971 13:37:09 0020002f 3980011693272A76
2023-02-01T22:33:30+0000 ttyS0
2023-02-01T22:34:09+0000 ttyS0   Audit on 1/5/1971 13:37:48 0020002f 3F4000339F8A2A77
2023-02-01T22:34:09+0000 ttyS0
2023-02-01T22:34:48+0000 ttyS0   Audit on 1/5/1971 13:38:27 0020002f 3F4000339F0A2A77
2023-02-01T22:34:48+0000 ttyS0
2023-02-01T22:35:30+0000 ttyS0   Audit on 1/5/1971 13:39:08 0020002f 3F4000339E8A2A77
2023-02-01T22:35:30+0000 ttyS0
2023-02-01T22:35:41+0000 ttyS0   Audit on 1/5/1971 13:39:20 00200063 3F4000339E8A2A77
2023-02-01T22:35:41+0000 ttyS0
2023-02-01T22:37:13+0000 ttyS0   Audit on 1/5/1971 13:40:52 0020002f 39800115FCA72A76
2023-02-01T22:37:13+0000 ttyS0
2023-02-01T22:38:03+0000 ttyS0   Audit on 1/5/1971 13:41:43 0020002f 39800115FC272A76
2023-02-01T22:38:03+0000 ttyS0
2023-02-01T22:38:15+0000 ttyS0   Audit on 1/5/1971 13:41:54 00200010 39800115FC272A76
2023-02-01T22:38:15+0000 ttyS0
2023-02-01T22:39:25+0000 ttyS0   Audit on 1/5/1971 13:43:04 0020006c
2023-02-01T22:39:25+0000 ttyS0
2023-02-01T22:39:52+0000 ttyS0   Audit on 1/5/1971 13:43:32 0020006b 39800115FD272A76
2023-02-01T22:39:52+0000 ttyS0
2023-02-01T22:40:29+0000 ttyS0   Audit on 1/5/1971 13:44:08 0020006b 3980011604A72A76
2023-02-01T22:40:29+0000 ttyS0
2023-02-01T22:41:02+0000 ttyS0   Audit on 1/5/1971 13:44:41 0020006b 3980011654672A76
2023-02-01T22:41:02+0000 ttyS0
2023-02-01T22:42:10+0000 ttyS0   Audit on 1/5/1971 13:45:49 0020006b 3980011620672A76
2023-02-01T22:42:10+0000 ttyS0
2023-02-01T22:42:40+0000 ttyS0   Audit on 1/5/1971 13:46:19 0020006b 39800115FAE72A76
2023-02-01T22:42:40+0000 ttyS0
2023-02-01T22:43:09+0000 ttyS0   Audit on 1/5/1971 13:46:48 0020006b 39800115F9E72A76
2023-02-01T22:43:09+0000 ttyS0
2023-02-01T22:44:06+0000 ttyS0   Audit on 1/5/1971 13:47:45 0020006b 39800115FAE72A76
2023-02-01T22:44:06+0000 ttyS0
2023-02-01T22:44:36+0000 ttyS0   Audit on 1/5/1971 13:48:16 0020006b 39800115F9E72A76
2023-02-01T22:44:36+0000 ttyS0
2023-02-01T22:45:00+0000 ttyS0   Audit on 1/5/1971 13:48:39 0020006b 398001161E272A76
2023-02-01T22:45:00+0000 ttyS0
```

```
2023-02-01T22:46:21+0000 ttyS0   Audit on 1/5/1971 13:50:00 0020006b 39800115FDA72A76
2023-02-01T22:46:21+0000 ttyS0
2023-02-01T22:46:53+0000 ttyS0   Audit on 1/5/1971 13:50:31 0020006b 398001160E272A76
2023-02-01T22:46:53+0000 ttyS0
2023-02-01T22:47:25+0000 ttyS0   Audit on 1/5/1971 13:51:04 0020006b 398001161FE72A76
2023-02-01T22:47:25+0000 ttyS0
2023-02-01T22:48:28+0000 ttyS0   Audit on 1/5/1971 13:52:08 0020002d 3F4000339E4A2A77
2023-02-01T22:48:28+0000 ttyS0
2023-02-01T22:49:18+0000 ttyS0   Audit on 1/5/1971 13:52:57 0020002d 3F4000339DCA2A77
2023-02-01T22:49:18+0000 ttyS0
2023-02-01T22:50:00+0000 ttyS0   Audit on 1/5/1971 13:53:39 0020002d 3980011693672A76
2023-02-01T22:50:00+0000 ttyS0
2023-02-01T22:50:44+0000 ttyS0   Audit on 1/5/1971 13:54:23 0020002d 3980011692272A76
2023-02-01T22:50:44+0000 ttyS0
2023-02-01T22:51:24+0000 ttyS0   Audit on 1/5/1971 13:55:03 0020002d 3F400031D2CA2A77
2023-02-01T22:51:24+0000 ttyS0
2023-02-01T22:52:04+0000 ttyS0   Audit on 1/5/1971 13:55:43 0020002d 3F400031D38A2A77
2023-02-01T22:52:04+0000 ttyS0
2023-02-01T22:52:46+0000 ttyS0   Audit on 1/5/1971 13:56:25 0020002d 3F400031D40A2A77
2023-02-01T22:52:46+0000 ttyS0
2023-02-01T22:55:27+0000 ttyS0   Audit on 1/5/1971 13:59:06 00200007
2023-02-01T22:55:27+0000 ttyS0
2023-02-01T22:56:18+0000 ttyS0   Audit on 1/5/1971 13:59:57 0020002d 3F4000339E0A2A77
2023-02-01T22:56:18+0000 ttyS0
2023-02-01T22:57:02+0000 ttyS0   Audit on 1/5/1971 14:00:42 0020002d 3F4000339D8A2A77
2023-02-01T22:57:02+0000 ttyS0
2023-02-01T22:57:42+0000 ttyS0   Audit on 1/5/1971 14:01:21 0020002d 3980011693E72A76
2023-02-01T22:57:42+0000 ttyS0
2023-02-01T22:58:22+0000 ttyS0   Audit on 1/5/1971 14:02:01 0020002d 3980011691A72A76
2023-02-01T22:58:22+0000 ttyS0
2023-02-01T22:59:01+0000 ttyS0   Audit on 1/5/1971 14:02:41 0020002d 3F400031D34A2A77
2023-02-01T22:59:01+0000 ttyS0
2023-02-01T22:59:42+0000 ttyS0   Audit on 1/5/1971 14:03:21 0020002d 3F400031D3CA2A77
2023-02-01T22:59:42+0000 ttyS0
2023-02-01T23:00:22+0000 ttyS0   Audit on 1/5/1971 14:04:01 0020002d 3F400031D44A2A77
2023-02-01T23:00:22+0000 ttyS0
2023-02-01T23:02:57+0000 ttyS0   Audit on 1/5/1971 14:06:36 00200007
2023-02-01T23:02:57+0000 ttyS0
2023-02-01T23:04:17+0000 ttyS0   Audit on 1/5/1971 14:07:56 00200069 3F4000339E8A2A77
2023-02-01T23:04:17+0000 ttyS0
2023-02-01T23:04:46+0000 ttyS0   Audit on 1/5/1971 14:08:25 00200069 3F4000339F0A2A77
2023-02-01T23:04:46+0000 ttyS0
2023-02-01T23:05:20+0000 ttyS0   Audit on 1/5/1971 14:08:59 00200069 3F4000339F8A2A77
2023-02-01T23:05:20+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0   TcpListener: Created IPv4 socket 19 on port 5000.
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0   TcpListener: Created IPv6 socket 21 on port 5000.
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:05:22+0000 ttyS0   Audit on 1/5/1971 14:09:01 00100002
2023-02-01T23:05:22+0000 ttyS0
2023-02-01T23:06:18+0000 ttyS0   Audit on 1/5/1971 14:09:57 00200069 3980011693272A76
2023-02-01T23:06:18+0000 ttyS0
2023-02-01T23:06:45+0000 ttyS0   Audit on 1/5/1971 14:10:24 00200069 4780000181AD2972
```

```
2023-02-01T23:06:45+0000        ttyS0
2023-02-01T23:07:09+0000        ttyS0   Audit on 1/5/1971 14:10:48 00200069 3F400033F88A2A77
2023-02-01T23:07:09+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0   TcpListener: Closed IPv4 socket 19 on port 5000.
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0   TcpListener: Closed IPv6 socket 21 on port 5000.
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:07:12+0000        ttyS0   Audit on 1/5/1971 14:10:51 00100003
2023-02-01T23:07:12+0000        ttyS0
2023-02-01T23:08:14+0000        ttyS0   Audit on 1/5/1971 14:11:53 00200069 4780000181AD2972
2023-02-01T23:08:14+0000        ttyS0
2023-02-01T23:08:36+0000        ttyS0   Audit on 1/5/1971 14:12:15 00200069 3F400033F88A2A77
2023-02-01T23:08:36+0000        ttyS0
2023-02-01T23:09:03+0000        ttyS0   Audit on 1/5/1971 14:12:42 00200069 3F400032D68A2A77
2023-02-01T23:09:03+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0   TcpListener: Created IPv4 socket 19 on port 5000.
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0   TcpListener: Created IPv6 socket 21 on port 5000.
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:09:06+0000        ttyS0   Audit on 1/5/1971 14:12:45 00100002
2023-02-01T23:09:06+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0   TcpListener: Accepted connection on socket 24 from address 192.168.0.1.
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0   CryptoTask: Closing connection on socket 24 from address 192.168.0.1.
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0   TcpListener: Accepted connection on socket 25 from address 192.168.0.1.
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:12:12+0000        ttyS0
2023-02-01T23:14:52+0000        ttyS0
2023-02-01T23:14:52+0000        ttyS0
2023-02-01T23:14:52+0000        ttyS0   CryptoTask: Closing connection on socket 25 from address 192.168.0.1.
2023-02-01T23:14:52+0000        ttyS0
2023-02-01T23:21:43+0000        ttyS0   Audit on 1/5/1971 14:25:22 00200069 3F4000339ECA2A77
2023-02-01T23:21:43+0000        ttyS0
2023-02-01T23:22:07+0000        ttyS0   Audit on 1/5/1971 14:25:46 00200069 3F4000339F4A2A77
2023-02-01T23:22:07+0000        ttyS0
2023-02-01T23:22:35+0000        ttyS0   Audit on 1/5/1971 14:26:13 00200069 3F4000339FCA2A77
2023-02-01T23:22:35+0000        ttyS0
2023-02-01T23:22:42+0000        ttyS0
2023-02-01T23:22:42+0000        ttyS0
2023-02-01T23:22:42+0000        ttyS0   TcpListener: Closed IPv4 socket 19 on port 5000.
2023-02-01T23:22:42+0000        ttyS0
2023-02-01T23:22:42+0000        ttyS0
2023-02-01T23:22:42+0000        ttyS0
```

```
2023-02-01T23:22:42+0000 ttyS0   TcpListener: Closed IPv6 socket 21 on port 5000.
2023-02-01T23:22:42+0000 ttyS0
2023-02-01T23:22:42+0000 ttyS0   Audit on 1/5/1971 14:26:21 00100003
2023-02-01T23:22:42+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   H2110017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   BBL CRC32: 0xDBC9B9F2
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   Running applicationBootLoader at 0xEFDC0000
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   H2110017 011403 ABL 030 : Tamper Challenge Response Key
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ABL CRC32: 0xE7E0FA6A
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ####################################
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ###     ABL tamper records        ###
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ####################################
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   Current Tamper Counts (decimal 0-255):
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ====================================
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   vextoosTamperCount:      0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   vintoosTamperCount:      4
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   vbboosTamperCount:       0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   maxstrtempTamperCount:   0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   minstrtempTamperCount:   0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   meshTamperCount:         0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   extampSMKTamperCount:    0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   extampIMKTamperCount:    0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   tempdiffTamperCount:     0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   pfTamperCount:           4
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   restartTamperCount:      10
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   Current tamper bitmaps:
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ======================
```

```
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   currentTamper bitmap:    0x0000 0b .... .... .... ....
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   lastTamper bitmap:       0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   Bitmapped Change Record (most recent first):
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0   ========================================
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:24+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0   Running cryptoApplication at 0xEBF00000
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0   Jumping to startup @ 0x001037B4
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0   Board is P2020RDB
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0   board_smp_init: 2 cpu
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0   Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:26+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0   System page at phys:0000b000 user:0000b000 kern:0000b000
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0   Starting next program at v0015183c
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0   Starting K-Series Kernel
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0   Copyright Ultra Electronics AEP. All Rights Reserved.
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0   Sat Jan 24 14:39:43 1970
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:27+0000 ttyS0   Starting auditd v2.0 ... started.
2023-02-01T23:55:27+0000 ttyS0
2023-02-01T23:55:28+0000 ttyS0   Interface 0 configured for IPv6.
2023-02-01T23:55:28+0000 ttyS0
2023-02-01T23:55:28+0000 ttyS0   Interface 0 configured for IPv4.
2023-02-01T23:55:28+0000 ttyS0
2023-02-01T23:55:28+0000 ttyS0   Interface 1 configured for IPv6.
2023-02-01T23:55:28+0000 ttyS0
2023-02-01T23:55:28+0000 ttyS0   Interface 1 configured for IPv4.
2023-02-01T23:55:28+0000 ttyS0
2023-02-01T23:55:28+0000 ttyS0   route: writing to routing socket: Network is unreachable
2023-02-01T23:55:29+0000 ttyS0
2023-02-01T23:55:29+0000 ttyS0   add net default: gateway ::: Network is unreachable
2023-02-01T23:55:29+0000 ttyS0
2023-02-01T23:55:29+0000 ttyS0   route: writing to routing socket: Network is unreachable
2023-02-01T23:55:29+0000 ttyS0
2023-02-01T23:55:29+0000 ttyS0   add net default: gateway 0.0.0.0: Network is unreachable
2023-02-01T23:55:29+0000 ttyS0
2023-02-01T23:55:29+0000 ttyS0   Starting USB driver...
2023-02-01T23:55:29+0000 ttyS0
```

```
2023-02-01T23:55:29+0000        ttyS0   9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-02-01T23:55:29+0000        ttyS0
2023-02-01T23:55:29+0000        ttyS0
2023-02-01T23:55:29+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   Running DES POST Test
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   DES POST Test Passed
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   Running Triple DES POST Test
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   Triple DES POST Test Passed
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   Running AES POST Test
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   AES POST Test Passed
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   Running SHA1 POST Test
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   SHA1 POST Test Passed
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   Running SHA2 POST Test
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:30+0000        ttyS0   SHA2 POST Test Passed
2023-02-01T23:55:30+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running RandomGen POST Test
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   RandomGen POST Test Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running RSA POST Test
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   RSA POST Test Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running DSA POST Test
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   DSA POST Test Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running SEED POST Test
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   SEED POST Test Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running RIPEMD160 POST Test
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   RIPEMD160 POST Test Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running ECC POST Test
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   ECC POST Test Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Running HMAC POST Tests
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   HMAC POST Tests Passed
2023-02-01T23:55:31+0000        ttyS0
2023-02-01T23:55:31+0000        ttyS0   Audit on 24/1/1970 14:39:46 00100008
```

```
2023-02-01T23:55:31+0000 ttyS0
2023-02-01T23:55:31+0000 ttyS0
2023-02-01T23:55:31+0000 ttyS0
2023-02-01T23:55:31+0000 ttyS0
2023-02-01T23:55:31+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Keyper 9860-2  Serial Number H2110017
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Memory Usage:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   RAM (free/total)          192Mb/256Mb
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Flash (free/total)        127Mb/128Mb
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0      black store            44b
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0      statistics             112b
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0      other                  116b
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   RedStore (free/total)    107Kb/128Kb
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Network Configuration:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Interface 0:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0       IPv4: enabled
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0       IPv6: enabled
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0       MAC/IP address(es): 00:E0:6C:00:C9:66 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c966/64
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Interface 1:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0       IPv4: enabled
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0       IPv6: enabled
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0       MAC/IP address(es): 00:E0:6C:00:C9:67 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c967/64
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   HSM Port 0: 05000
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   HSM Port 1: 03000
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Default Gateway(s): 0.0.0.0 ::
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Software Versions:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   BBL 030 ABL 021 App 034
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
```

```
2023-02-01T23:55:32+0000 ttyS0   CPLD Version:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   1.9
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   SCR Firmware Version:
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   OROS-R2.99-R1.20
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:55:32+0000 ttyS0   Audit on 24/1/1970 14:39:47 00100001
2023-02-01T23:55:32+0000 ttyS0
2023-02-01T23:56:54+0000 ttyS0   Audit on 24/1/1970 14:41:10 00200035 39800115FCA72A76
2023-02-01T23:56:54+0000 ttyS0
2023-02-01T23:57:12+0000 ttyS0   Audit on 24/1/1970 14:41:28 00200035 39800115FC272A76
2023-02-01T23:57:12+0000 ttyS0
2023-02-01T23:57:13+0000 ttyS0   Audit on 24/1/1970 14:41:28 0020000e 39800115FC272A76
2023-02-01T23:57:13+0000 ttyS0
2023-02-01T23:58:25+0000 ttyS0   Audit on 24/1/1970 14:42:41 0020002f 3F400031D50A2A77
2023-02-01T23:58:25+0000 ttyS0
2023-02-01T23:59:04+0000 ttyS0   Audit on 24/1/1970 14:43:20 0020002f 3F400031D58A2A77
2023-02-01T23:59:04+0000 ttyS0
2023-02-02T00:00:10+0000 ttyS0   Audit on 24/1/1970 14:44:25 0020002f 3F400031CF4A2A77
2023-02-02T00:00:10+0000 ttyS0
2023-02-02T00:00:50+0000 ttyS0   Audit on 24/1/1970 14:45:06 0020002f 3F400031D10A2A77
2023-02-02T00:00:50+0000 ttyS0
2023-02-02T00:01:30+0000 ttyS0   Audit on 24/1/1970 14:45:46 0020002f 3F400031D1CA2A77
2023-02-02T00:01:30+0000 ttyS0
2023-02-02T00:02:10+0000 ttyS0   Audit on 24/1/1970 14:46:26 0020002f 3980011646272A76
2023-02-02T00:02:10+0000 ttyS0
2023-02-02T00:02:49+0000 ttyS0   Audit on 24/1/1970 14:47:05 0020002f 39800115F5672A76
2023-02-02T00:02:49+0000 ttyS0
2023-02-02T00:03:01+0000 ttyS0   Audit on 24/1/1970 14:47:16 00200019 39800115F5672A76
2023-02-02T00:03:01+0000 ttyS0
2023-02-02T00:05:01+0000 ttyS0   Audit on 24/1/1970 14:49:16 0020002f 3F400031D54A2A77
2023-02-02T00:05:01+0000 ttyS0
2023-02-02T00:05:37+0000 ttyS0   Audit on 24/1/1970 14:49:53 0020002f 3F400031D5CA2A77
2023-02-02T00:05:37+0000 ttyS0
2023-02-02T00:06:11+0000 ttyS0   Audit on 24/1/1970 14:50:27 0020002f 3F400031D04A2A77
2023-02-02T00:06:11+0000 ttyS0
2023-02-02T00:06:45+0000 ttyS0   Audit on 24/1/1970 14:51:01 0020002f 3F400031D18A2A77
2023-02-02T00:06:45+0000 ttyS0
2023-02-02T00:07:21+0000 ttyS0   Audit on 24/1/1970 14:51:37 0020002f 3F400031D24A2A77
2023-02-02T00:07:21+0000 ttyS0
2023-02-02T00:07:58+0000 ttyS0   Audit on 24/1/1970 14:52:14 0020002f 39800115F5A72A76
2023-02-02T00:07:58+0000 ttyS0
2023-02-02T00:08:32+0000 ttyS0   Audit on 24/1/1970 14:52:48 0020002f 39800115F4E72A76
2023-02-02T00:08:32+0000 ttyS0
2023-02-02T00:08:44+0000 ttyS0   Audit on 24/1/1970 14:52:59 00200019 39800115F4E72A76
2023-02-02T00:08:44+0000 ttyS0
2023-02-02T00:09:55+0000 ttyS0   Audit on 24/1/1970 14:54:10 00200023 39800115F4E72A76
2023-02-02T00:09:55+0000 ttyS0
2023-02-02T00:10:24+0000 ttyS0   Audit on 24/1/1970 14:54:39 00200023 39800115F5A72A76
2023-02-02T00:10:24+0000 ttyS0
2023-02-02T00:10:58+0000 ttyS0   Audit on 24/1/1970 14:55:13 00200023 3F400031D24A2A77
```

```
2023-02-02T00:10:58+0000 ttyS0
2023-02-02T00:11:10+0000 ttyS0   Audit on 24/1/1970 14:55:25 00200056
2023-02-02T00:11:10+0000 ttyS0
2023-02-02T00:11:35+0000 ttyS0   Audit on 24/1/1970 14:55:50 00200081
2023-02-02T00:11:35+0000 ttyS0
2023-02-02T00:11:47+0000 ttyS0   Audit on 24/1/1970 14:56:03 00200054
2023-02-02T00:11:47+0000 ttyS0
2023-02-02T00:11:51+0000 ttyS0   Audit on 24/1/1970 14:56:06 00200028
2023-02-02T00:11:51+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   HmcListener: Created IPv4 socket 9 on port 3000.
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   HmcListener: Created IPv6 socket 11 on port 3000.
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   Audit on 24/1/1970 14:56:10 00100003
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   Audit on 24/1/1970 14:56:10 00100005
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   Shutting down daemons...
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   AuditBuffer rx'd [-1] (3)
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   shutting down audit service.
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:55+0000 ttyS0   Terminated
2023-02-02T00:11:55+0000 ttyS0
2023-02-02T00:11:56+0000 ttyS0   HmcListener::accept(): No such process
2023-02-02T00:11:56+0000 ttyS0
2023-02-02T00:11:56+0000 ttyS0   Shutting down filesystems...
2023-02-02T00:11:56+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   H2110017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   BBL CRC32: 0xDBC9B9F2
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   Running applicationBootLoader at 0xEFDC0000
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   H2110017 011403 ABL 030 : Tamper Challenge Response Key
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   ABL CRC32: 0xE7E0FA6A
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   ####################################
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   ###     ABL tamper records        ###
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   ####################################
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0   Current Tamper Counts (decimal 0-255):
2023-02-02T00:11:58+0000 ttyS0
```

```
2023-02-02T00:11:58+0000 ttyS0 ================================
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 vextoosTamperCount:      0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 vintoosTamperCount:      4
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 vbboosTamperCount:       0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 maxstrtempTamperCount:   0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 minstrtempTamperCount:   0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 meshTamperCount:         0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 extampSMKTamperCount:    0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 extampIMKTamperCount:    0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 tempdiffTamperCount:     0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 pfTamperCount:           4
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 restartTamperCount:      10
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 Current tamper bitmaps:
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 ====================
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 currentTamper bitmap:    0x0000 0b .... .... .... ....
2023-02-02T00:11:58+0000 ttyS0 lastTamper bitmap:       0x0080 0b .... .... 1... ....  |EXT_POWER_DOWN
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 Bitmapped Change Record (most recent first):
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 ======================================
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0
2023-02-02T00:11:58+0000 ttyS0 Running cryptoApplication at 0xEBF00000
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0 Jumping to startup @ 0x001037B4
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0 Board is P2020RDB
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0 board_smp_init: 2 cpu
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0 Cpu_clk=1000000000, Sys_clk=100000000, CCB=500000000
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:11:59+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0 System page at phys:0000b000 user:0000b000 kern:0000b000
```

```
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0    Starting next program at v0015183c
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0    Starting K-Series Kernel
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0    Copyright Ultra Electronics AEP. All Rights Reserved.
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0    Sat Jan 24 14:56:17 1970
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0    Starting auditd v2.0 ... started.
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:01+0000 ttyS0    Interface 0 configured for IPv6.
2023-02-02T00:12:01+0000 ttyS0
2023-02-02T00:12:02+0000 ttyS0    Interface 0 configured for IPv4.
2023-02-02T00:12:02+0000 ttyS0
2023-02-02T00:12:02+0000 ttyS0    Interface 1 configured for IPv6.
2023-02-02T00:12:02+0000 ttyS0
2023-02-02T00:12:02+0000 ttyS0    Interface 1 configured for IPv4.
2023-02-02T00:12:02+0000 ttyS0
2023-02-02T00:12:02+0000 ttyS0    route: writing to routing socket: Network is unreachable
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0    add net default: gateway ::: Network is unreachable
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0    route: writing to routing socket: Network is unreachable
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0    add net default: gateway 0.0.0.0: Network is unreachable
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0    Starting USB driver...
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0    9860 v3.4 Keyper Application - May 19 2017 15:48:58
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:03+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Running DES POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    DES POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Running Triple DES POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Triple DES POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Running AES POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    AES POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Running SHA1 POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    SHA1 POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Running SHA2 POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    SHA2 POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0    Running RandomGen POST Test
2023-02-02T00:12:04+0000 ttyS0
```

```
2023-02-02T00:12:04+0000 ttyS0   RandomGen POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   Running RSA POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   RSA POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   Running DSA POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   DSA POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   Running SEED POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   SEED POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   Running RIPEMD160 POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   RIPEMD160 POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   Running ECC POST Test
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   ECC POST Test Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   Running HMAC POST Tests
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0   HMAC POST Tests Passed
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:04+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   Keyper 9860-2  Serial Number H2110017
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   Memory Usage:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   RAM (free/total)          192Mb/256Mb
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   Flash (free/total)        127Mb/128Mb
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      black store            272b
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      statistics             112b
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      other                  116b
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   RedStore (free/total)     107Kb/128Kb
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   Network Configuration:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0   Interface 0:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      IPv4: enabled
```

```
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      IPv6: enabled
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      MAC/IP address(es): 00:E0:6C:00:C9:66 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c966/64
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  Interface 1:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      IPv4: enabled
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      IPv6: enabled
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0      MAC/IP address(es): 00:E0:6C:00:C9:67 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c967/64
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  HSM Port 0: 05000
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  HSM Port 1: 03000
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  Default Gateway(s): 0.0.0.0 ::
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  Software Versions:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  BBL 030 ABL 021 App 034
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  CPLD Version:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  1.9
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  SCR Firmware Version:
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  OROS-R2.99-R1.20
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  HmcListener: Created IPv4 socket 9 on port 3000.
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  HmcListener: Created IPv6 socket 10 on port 3000.
2023-02-02T00:12:05+0000 ttyS0
2023-02-02T00:12:05+0000 ttyS0  Audit on 24/1/1970 14:56:21 00100003
2023-02-02T00:12:06+0000 ttyS0
2023-02-02T00:12:06+0000 ttyS0  Audit on 24/1/1970 14:57:12 00200023 3F400031D18A2A77
2023-02-02T00:12:56+0000 ttyS0
2023-02-02T00:12:56+0000 ttyS0  Audit on 24/1/1970 14:57:38 00200023 3F400031D04A2A77
2023-02-02T00:13:22+0000 ttyS0
2023-02-02T00:13:22+0000 ttyS0  Audit on 24/1/1970 14:58:01 00200023 3F400031D5CA2A77
2023-02-02T00:13:46+0000 ttyS0
2023-02-02T00:13:46+0000 ttyS0  Audit on 24/1/1970 14:58:48 00200023 3F400031D04A2A77
2023-02-02T00:14:32+0000 ttyS0
2023-02-02T00:14:32+0000 ttyS0
```

```
2023-02-02T00:14:54+0000 ttyS0   Audit on 24/1/1970 14:59:10 00200023 3F400031D5CA2A77
2023-02-02T00:14:54+0000 ttyS0
2023-02-02T00:15:18+0000 ttyS0   Audit on 24/1/1970 14:59:34 00200023 3F400031D54A2A77
2023-02-02T00:15:18+0000 ttyS0
2023-02-02T00:16:01+0000 ttyS0   Audit on 24/1/1970 15:00:17 00200023 39800115F5672A76
2023-02-02T00:16:01+0000 ttyS0
2023-02-02T00:16:25+0000 ttyS0   Audit on 24/1/1970 15:00:41 00200023 3980011646272A76
2023-02-02T00:16:25+0000 ttyS0
2023-02-02T00:16:48+0000 ttyS0   Audit on 24/1/1970 15:01:04 00200023 3F400031D1CA2A77
2023-02-02T00:16:48+0000 ttyS0
2023-02-02T00:17:27+0000 ttyS0   Audit on 24/1/1970 15:01:42 00200023 3F400031D10A2A77
2023-02-02T00:17:27+0000 ttyS0
2023-02-02T00:17:50+0000 ttyS0   Audit on 24/1/1970 15:02:06 00200023 3F400031CF4A2A77
2023-02-02T00:17:50+0000 ttyS0
2023-02-02T00:18:13+0000 ttyS0   Audit on 24/1/1970 15:02:29 00200023 3F400031D58A2A77
2023-02-02T00:18:13+0000 ttyS0
2023-02-02T00:19:10+0000 ttyS0   Audit on 24/1/1970 15:03:26 0020006b 3980011620E72A76
2023-02-02T00:19:10+0000 ttyS0
2023-02-02T00:19:33+0000 ttyS0   Audit on 24/1/1970 15:03:49 0020006b 39800115FA272A76
2023-02-02T00:19:33+0000 ttyS0
2023-02-02T00:19:58+0000 ttyS0   Audit on 24/1/1970 15:04:13 0020006b 398001161EA72A76
2023-02-02T00:19:58+0000 ttyS0
2023-02-02T00:20:19+0000 ttyS0   Audit on 24/1/1970 15:04:35 00200039
2023-02-02T00:20:19+0000 ttyS0
2023-02-02T00:20:28+0000 ttyS0   Audit on 24/1/1970 15:04:44 0020003b
2023-02-02T00:20:28+0000 ttyS0
2023-02-02T00:20:39+0000 ttyS0   Audit on 24/1/1970 15:04:55 00200041
2023-02-02T00:20:39+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   HSM Status
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   ==================
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Keyper 9860-2
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Serial Number H2110017
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Date(dd/mm/yyyy) 24/1/1970  Time 15:5:34
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Software Versions:
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   BBL 030 ABL 021 App 034
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   CPLD Version:
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   1.9
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
```

```
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   SCR Firmware Version:
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   OROS-R2.99-R1.20
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Memory Usage:
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   RAM (free/total)         192Mb/256Mb
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Flash (free/total)       127Mb/128Mb
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0      black store           452b
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0      statistics            112b
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0      other                 116b
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   RedStore (free/total)    107Kb/128Kb
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Network Configuration:
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   Interface 0:
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0       IPv4: enabled
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0       IPv6: enabled
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0       MAC/IP address(es): 00:E0:6C:00:C9:66 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c966/64
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0   tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2023-02-02T00:21:18+0000 ttyS0
2023-02-02T00:21:18+0000 ttyS0           capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           capabilities tx=0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           enabled=0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           address: 00:e0:6c:00:c9:66
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           media: Ethernet none
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           inet6 2001::2e0:6cff:fe00:c966 prefixlen 64
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0           inet6 fe80::2e0:6cff:fe00:c966%tsec0 prefixlen 64 scopeid 0x2
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
```

```
2023-02-02T00:21:19+0000 ttyS0  Interface 1:
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0      IPv4: enabled
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0      IPv6: enabled
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0      MAC/IP address(es): 00:E0:6C:00:C9:67 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c967/64
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  tsec1: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          capabilities tx=0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          enabled=0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          address: 00:e0:6c:00:c9:67
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          media: Ethernet none
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          inet 192.168.1.2 netmask 0xffffff00 broadcast 192.168.1.255
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          inet6 2001::1:2e0:6cff:fe00:c967 prefixlen 64
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0          inet6 fe80::2e0:6cff:fe00:c967%tsec1 prefixlen 64 scopeid 0x3
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  HSM Port 0: 05000
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  HSM Port 1: 03000
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Default Gateway(s): 0.0.0.0 ::
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Current HSM State: Secured Off-line
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Modes: (1=Enabled 0=Disabled)
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Global Key Export     1  App Key Import        0  App Key Export        0  Asymmetric Key Gen    1
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Symmetric Key Gen     1  Symmetric Key Derive  0  Signing               1  Signature Verify      1
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  MAC Generation        1  MAC Verification      1  Encrypt / Decrypt     1  Delete Asym Key       1
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Delete Sym Key        1  Output Key Details    1  Output Key Summary    1  Suite B Algorithms    1
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Non Suite B Algs      1  Auto Online           0  Remote Management     0
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  Other Modes:
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0  AES SMK                  Set Offline             FIPS Mode
2023-02-02T00:21:19+0000 ttyS0
2023-02-02T00:21:19+0000 ttyS0
```

```
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   Battery ok
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   ####################################
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   ###     ABL tamper records       ###
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   ####################################
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   Current Tamper Counts (decimal 0-255):
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   ====================================
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   vextoosTamperCount:     0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   vintoosTamperCount:     0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   vbboosTamperCount:      0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   maxstrtempTamperCount:  0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   minstrtempTamperCount:  0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   meshTamperCount:        0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   extampSMKTamperCount:   0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   extampIMKTamperCount:   0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   tempdiffTamperCount:    0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   pfTamperCount:          0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   restartTamperCount:     0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   Current tamper bitmaps:
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   ====================
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   currentTamper bitmap:   0x0000 0b .... .... .... ....
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   lastTamper bitmap:      0x0000 0b .... .... .... ....
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   Bitmapped Change Record (most recent first):
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   ====================================
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   \000====================================
2023-02-02T00:21:19+0000        ttyS0
```

```
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   DRBG Instantiate Health Test On Demand Passed
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   DRBG Generate Health Test On Demand Passed
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:21:19+0000        ttyS0   DRBG Reseed Health Test On Demand Passed
2023-02-02T00:21:19+0000        ttyS0
2023-02-02T00:26:44+0000        ttyS0   Audit on 24/1/1970 15:11:00 0020006b 39800115FA272A76
2023-02-02T00:26:44+0000        ttyS0
2023-02-02T00:27:06+0000        ttyS0   Audit on 24/1/1970 15:11:22 0020006b 398001161EA72A76
2023-02-02T00:27:06+0000        ttyS0
2023-02-02T00:27:31+0000        ttyS0   Audit on 24/1/1970 15:11:46 0020006b 398001161DA72A76
2023-02-02T00:27:31+0000        ttyS0
2023-02-02T00:28:26+0000        ttyS0   Audit on 24/1/1970 15:12:42 00200025 3F400031D44A2A77
2023-02-02T00:28:26+0000        ttyS0
2023-02-02T00:28:49+0000        ttyS0   Audit on 24/1/1970 15:13:05 00200025 3F400031D3CA2A77
2023-02-02T00:28:49+0000        ttyS0
2023-02-02T00:29:14+0000        ttyS0   Audit on 24/1/1970 15:13:30 00200025 3F400031D34A2A77
2023-02-02T00:29:14+0000        ttyS0
2023-02-02T00:29:17+0000        ttyS0   Audit on 24/1/1970 15:13:32 00200005
2023-02-02T00:29:17+0000        ttyS0
2023-02-02T00:31:00+0000        ttyS0   Audit on 24/1/1970 15:15:16 00200016 Klajeyz
2023-02-02T00:31:00+0000        ttyS0
2023-02-02T00:31:00+0000        ttyS0   Audit on 24/1/1970 15:15:16 00200015 47800001806D2972
2023-02-02T00:31:00+0000        ttyS0
2023-02-02T00:31:00+0000        ttyS0   Audit on 24/1/1970 15:15:16 00200018
2023-02-02T00:31:00+0000        ttyS0
2023-02-02T00:34:00+0000        ttyS0   Audit on 24/1/1970 15:18:16 00200069 3980011692A72A76
2023-02-02T00:34:00+0000        ttyS0
2023-02-02T00:34:26+0000        ttyS0   Audit on 24/1/1970 15:18:41 00200069 3F400031D48A2A77
2023-02-02T00:34:26+0000        ttyS0
2023-02-02T00:34:49+0000        ttyS0   Audit on 24/1/1970 15:19:05 00200069 3F400032D70A2A77
2023-02-02T00:34:49+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0   TcpListener: Created IPv4 socket 20 on port 5000.
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0   TcpListener: Created IPv6 socket 21 on port 5000.
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:34:51+0000        ttyS0   Audit on 24/1/1970 15:19:07 00100002
2023-02-02T00:34:51+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0   TcpListener: Accepted connection on socket 22 from address 192.168.0.1.
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0   CryptoTask: Closing connection on socket 22 from address 192.168.0.1.
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:37:23+0000        ttyS0   TcpListener: Accepted connection on socket 22 from address 192.168.0.1.
```

```
2023-02-02T00:37:23+0000        ttyS0
2023-02-02T00:38:47+0000        ttyS0
2023-02-02T00:38:47+0000        ttyS0
2023-02-02T00:38:47+0000        ttyS0   CryptoTask: Closing connection on socket 22 from address 192.168.0.1.
2023-02-02T00:38:47+0000        ttyS0
2023-02-02T00:43:02+0000        ttyS0   Audit on 24/1/1970 15:27:18 00200069 3F400031D48A2A77
2023-02-02T00:43:02+0000        ttyS0
2023-02-02T00:43:28+0000        ttyS0   Audit on 24/1/1970 15:27:44 00200069 3F400032D70A2A77
2023-02-02T00:43:28+0000        ttyS0
2023-02-02T00:43:50+0000        ttyS0   Audit on 24/1/1970 15:28:05 00200069 3F400032D64A2A77
2023-02-02T00:43:50+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0   TcpListener: Closed IPv4 socket 20 on port 5000.
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0   TcpListener: Closed IPv6 socket 21 on port 5000.
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:43:54+0000        ttyS0   Audit on 24/1/1970 15:28:09 00100003
2023-02-02T00:43:54+0000        ttyS0
2023-02-02T00:44:56+0000        ttyS0   Audit on 24/1/1970 15:29:12 00200023 3F400031CF4A2A77
2023-02-02T00:44:56+0000        ttyS0
2023-02-02T00:45:20+0000        ttyS0   Audit on 24/1/1970 15:29:36 00200023 3F400031D58A2A77
2023-02-02T00:45:20+0000        ttyS0
2023-02-02T00:45:47+0000        ttyS0   Audit on 24/1/1970 15:30:03 00200023 3F400031D50A2A77
2023-02-02T00:45:47+0000        ttyS0
2023-02-02T00:46:54+0000        ttyS0   Audit on 24/1/1970 15:31:10 0020002c 39800115FCA72A76
2023-02-02T00:46:54+0000        ttyS0
2023-02-02T00:47:31+0000        ttyS0   Audit on 24/1/1970 15:31:47 0020002c 39800115FC272A76
2023-02-02T00:47:31+0000        ttyS0
```

# Prepare blank FDs and back up the HSMFD Contents

| Step | Activity | Initials | Time |
|---|---|---|---|
| 3 | CA executes the command below using the terminal window to enable copying of all content from the HSMFD:<br>`shopt -s dotglob` | JD | 01:00 |
| 4 | CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content:<br>a) `lpadmin -p HP -o copies-default=2`<br>b) `hsmfd-hash -p`<br>**Note: One copy for audit bundle and one copy for HSMFD package.** | JD | 01:01 |
| 5 | CA executes the command below using the terminal window to display the contents of the HSMFD:<br>`ls -ltrR` | JD | 01:02 |
| 6 | CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs:<br>`mkdir /media/HSMFD1` | JD | 01:02 |
| 7 | CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it. | JD | 01:03 |
| 8 | CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD:<br>`df` | JD | 01:03 |
| 9 | CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD:<br>a) `umount /dev/sdc1`<br>b) `mkfs.vfat -n HSMFD -I /dev/sdc1`<br>c) `mount /dev/sdc1 /media/HSMFD1`<br>d) `cp -pR * /media/HSMFD1` | JD | 01:04 |
| 10 | 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:<br>a) `hsmfd-hash -m`<br>b) `umount /media/HSMFD1` | JD | 01:05 |
| 11 | CA removes the **HSMFD copy**, then places it on the holder.<br>**Wait for the activity light on the backup HSMFD to stop flashing before removal.** | JD | 01:05 |
| 12 | CA repeats step 7 to 11 for the 2nd copy.<br>**Wait for the activity light on the backup HSMFD to stop flashing before executing each step.** | JD | 01:06 |
| 13 | CA repeats step 7 to 11 for the 3rd copy.<br>**Wait for the activity light on the backup HSMFD to stop flashing before executing each step.** | JD | 01:07 |
| 14 | CA repeats step 7 to 11 for the 4th copy.<br>**Wait for the activity light on the backup HSMFD to stop flashing before executing each step.** | JD | 01:08 |
| 15 | CA repeats step 7 to 11 for the 5th copy.<br>**Wait for the activity light on the backup HSMFD to stop flashing before executing each step.** | JD | 01:08 |

**HSMFD SHA-256 HASH** **2023/02/02**

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

SHA-256:    3dc08e54e71b2097beed6ad35acbe7b7f9c3ca8c2c147a636d93b15f2a6edd30
PGP Words:  commence recipe orca equation transit bravado bison mosquito skydive unify Geig
er sociable enlist revival transit processor waffle replica spellbind megaton Burbank below
ground keyboard Galveston goggles molasses sailboat forever brickyard headwaters swelter co
mmando
```

## 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:<br>a) `cd /tmp`<br>b) `umount /media/HSMFD`<br>CA removes the HSMFD, then places it on the holder. | JD | 01:09 |
| 17 | CA performs the following steps to switch OFF the laptop and remove the OS DVD:<br>a) Remove the OS DVD from the laptop.<br>b) Turn OFF the laptop by pressing the power button.<br>c) Disconnect all connections from the laptop. | JD | 01:10 |
| 18 | CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seals it. | JD | 01:11 |
| 19 | CA performs the following steps to verify the TEB:<br>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number matches with the information below.<br>c) Initial the TEB along with IW using a ballpoint pen.<br>d) Give IW the sealing strips for post-ceremony inventory.<br>e) Place the OS DVD TEB on the cart.<br><br>**OS DVD (release coen-0.4.0) + HSMFD: TEB # BB02638569** | JD | 01:11 |
| 20 | CA distributes the remaining HSMFDs:<br>2 for IW (for audit bundles).<br>2 for RKOS (for SKR exchange with RZM and process review). | JD | 01:12 |

## Place the Laptop into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 21 | CA places the laptop into its designated new TEB, then seals it. | JD | 01:13 |
| 22 | CA performs the following steps:<br>a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number and laptop serial number matches with the information below.<br>c) Initial the TEB along with IW using a ballpoint pen.<br>d) Give IW the sealing strips for post-ceremony inventory.<br>e) Place the laptop TEB on the cart.<br><br>**Laptop3: TEB # BB97448420 / Service Tag # C8SVSG2** | JD | 01:13 |

# 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:<br>a) CA takes the TEB and plastic case prepared for the CO.<br>b) CO takes their cards from the card holder and places them inside the plastic case.<br>c) CO gives the plastic case containing the cards to the CA.<br>d) CA places the plastic case into its designated new TEB, reads aloud the TEB number and description, then seals it.<br>e) CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony inventory.<br>f) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.<br>g) CA gives the TEB containing the cards to the CO.<br>h) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen.<br>i) CO writes the date and time, then signs the table of the IW's script, then the IW initials the entry.<br>j) CO returns to their seat with their TEBs, being especially careful not to compromise any TEB.<br>k) Repeat steps for all the remaining COs' credentials on the list.<br><br>**CO1: Arbogast Fabian**<br>**SET1 TEB # BB02638562**<br>**SET2 TEB # BB02638561**<br><br>**CO2: Ralf Weber**<br>**OP TEB # BB02638566**<br>**SO TEB # BB02638565**<br>**SET1 TEB # BB02638560**<br>**SET2 TEB # BB02638559**<br><br>**CO3: João Damas**<br>**SET1 TEB # BB02638558**<br>**SET2 TEB # BB02638557**<br><br>**CO4: Carlos Martinez**<br>**SO TEB # BB02638564**<br>**SET1 TEB # BB02638556**<br>**SET2 TEB # BB02638555**<br><br>**CO5: Ólafur Guðmundsson**<br>**SO TEB # BB02638563**<br>**SET1 TEB # BB02638554**<br>**SET2 TEB # BB02638553**<br><br>**CO6: Jorge Etges**<br>**SET1 TEB # BB02638552**<br>**SET2 TEB # BB02638551**<br><br>**CO7: Subramanian Moonesamy**<br>**SET1 TEB # BB02638550**<br>**SET2 TEB # BB02638549** | JD | 10:41 |

| CO | TEB # | Printed Name | Signature | Date | Time | IW Initials |
|---|---|---|---|---|---|---|
| CO1 | SET1 TEB # **BB02638562**<br>SET2 TEB # **BB02638561** | **Arbogast Fabian** | | **2023 Feb** 02 | 01:20 | JD |
| CO2 | OP TEB # **BB02638566**<br>SO TEB # **BB02638565**<br>SET1 TEB # **BB02638560**<br>SET2 TEB # **BB02638559** | **Ralf Weber** | | **2023 Feb** 02 | 01:25 | JD |
| CO3 | SET1 TEB # **BB02638558**<br>SET2 TEB # **BB02638557** | **João Damas** | | **2023 Feb** 02 | 01:28 | JD |
| CO4 | SO TEB # **BB02638564**<br>SET1 TEB # **BB02638556**<br>SET2 TEB # **BB02638555** | **Carlos Martinez** | | **2023 Feb** 02 | 01:32 | JD |
| CO5 | SO TEB # **BB02638563**<br>SET1 TEB # **BB02638554**<br>SET2 TEB # **BB02638553** | **Ólafur Guðmundsson** | | **2023 Feb** 02 | 01:35 | JD |
| CO6 | SET1 TEB # **BB02638552**<br>SET2 TEB # **BB02638551** | **Jorge Etges** | | **2023 Feb** 2 | 01:38 | JD |
| CO7 | SET1 TEB # **BB02638550**<br>SET2 TEB # **BB02638549** | **Subramanian Moonesamy** | | **2023 Feb** 2 | 01:41 | JD |

# Root DNSSEC Script Exception

## Exception Details

| Step | Activity | Initials | Time |
|---|---|---|---|
| 1 | IW writes the details of the ceremony exception:<br>Act: 6 Step(s): 27 Page(s): 40<br>Date and Time: 02-02-2023 01:50<br>**Note: IW describes the exception(s) and action(s) below.** | JD | 01:50 |

DUE TO THE EXCEPTION THAT OCCURRED FROM ACT 5, STEP 36, THE LOG FILES FOR SAFE H1 HAD TO BE UPDATED BY HAND TO ACCOUNT FOR THE TPB CHANGE.

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

| Step | Activity | Initials | Time |
|---|---|---|---|
| 24 | CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.) | JD | 01:42 |
| 25 | SSC1 opens Safe #1 while shielding the combination from the camera.<br>**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.** | JD | 01:44 |
| 26 | SSC1 removes the safe log, then writes the date and time, then signs the safe log where **"Open Safe"** is indicated.<br>IW verifies this entry, then initials it.<br>**Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** | JD | 01:44 |
| 27 | CA performs the following steps to return each piece of equipment to the safe:<br>a) CAREFULLY remove the equipment TEB from the cart.<br>b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1<br>c) Write the date, time, and signature on the safe log where **"Return"** is indicated.<br>d) IW verifies the safe log entry, then initials it.<br><br>**HSM6W: TEB # BB51184545**<br>**HSM7W: TEB # ~~BB51184546~~** NEW TEB # BB51184520<br>**Laptop3: TEB # BB97448420**<br>**OS DVD (release coen-0.4.0) + HSMFD: TEB # BB02638569**<br>**KSK-2017: TEB # BB02638568** | JD | 01:50 |

## Close Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 28 | SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it. | JD | 01:50 |
| 29 | SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off. | JD | 01:51 |
| 30 | CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room). | JD | 01:51 |

## Open Safe #2 (Tier 6, Credentials Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 31 | CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.) | JD | 01:54 |
| 32 | SSC2 opens Safe #2 while shielding the combination from the camera.<br>**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.** | JD | 01:55 |
| 33 | SSC2 removes the safe log, then writes the date and time, then signs the safe log where **"Open Safe"** is indicated.<br>IW verifies this entry, then initials it.<br>**Note: If log entry is pre-printed, verify the entry, record time of completion and sign.** | JD | 01:56 |

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

| Step | Activity | Initials | Time |
|---|---|---|---|
| 34 | COs perform the following steps sequentially to return the listed TEBs:<br>a) CO reads aloud the TEB number(s), then verifies integrity while showing the TEB(s) to the audit camera above<br>b) After the CA operates the guard key in the bottom lock, CO reads aloud the safe deposit box number and uses their tenant key to operate the top lock.<br>c) CO opens their safe deposit box, places their TEB(s) inside, then closes and locks the safe deposit box.<br>d) CO writes the date and time, then signs the safe log where **"Return"** is indicated.<br>e) IW verifies the completed safe log entry, then initials it.<br><br>**CO1: Arbogast Fabian**<br>**Box # 1788**<br>**SET1 TEB # BB02638562**<br>**SET2 TEB # BB02638561**<br><br>**CO2: Ralf Weber**<br>**Box # 1071**<br>**OP TEB # BB02638566**<br>**SO TEB # BB02638565**<br>**SET1 TEB # BB02638560**<br>**SET2 TEB # BB02638559**<br><br>**CO3: João Damas**<br>**Box # 1069**<br>**SET1 TEB # BB02638558**<br>**SET2 TEB # BB02638557**<br><br>**CO4: Carlos Martinez**<br>**Box # 1073**<br>**SO TEB # BB02638564**<br>**SET1 TEB # BB02638556**<br>**SET2 TEB # BB02638555**<br><br>**CO5: Ólafur Guðmundsson**<br>**Box # 1070**<br>**SO TEB # BB02638563**<br>**SET1 TEB # BB02638554**<br>**SET2 TEB # BB02638553**<br><br>**CO6: Jorge Etges**<br>**Box # 1072**<br>**SET1 TEB # BB02638552**<br>**SET2 TEB # BB02638551**<br><br>**CO7: Subramanian Moonesamy**<br>**Box # 1790**<br>**SET1 TEB # BB02638550**<br>**SET2 TEB # BB02638549** | JD | 02:09 |

# Close Safe #2 (Tier 6, Credentials Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 35 | Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry, then initials it. | JD | 02:10 |
| 36 | SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off. | JD | 02:10 |
| 37 | CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room). | JD | 02:11 |

# 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. | JD | 02:14 |
| 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.** | JD | 02:21 |
| 3 | CA reviews IW's script, then signs the participants list. | JD | 02:23 |
| 4 | IW signs the list and records the completion time. | JD | 02:23 |

## Stop Online Streaming and Recording

| Step | Activity | Initials | Time |
|---|---|---|---|
| 5 | CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming. | JD | 02:23 |
| 6 | CA requests that an SA stop the audit camera video recording. | JD | 02:24 |
| 7 | CA informs onsite participants of post ceremony activities. | JD | 02:24 |
| 8 | Ceremony participants take a group photo. | JD | 02:26 |

## Sign Out of Tier 4 (Key Ceremony Room)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 9 | RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.) SA, IW, and CA must remain in Tier 4 (Key Ceremony Room.) | JD | 02:35 |

## Bundle Audit Materials

| Step | Activity | Initials | Time |
|---|---|---|---|
| 10 | IW makes a copy of their script for off-site audit bundle containing:<br>a) Output of signer system – HSMFD.<br>b) Copy of IW's key ceremony script.<br>c) Audio-visual recording from the audit cameras.<br>d) Logs from the Physical Access Control System and Intrusion Detection System:<br>Range: **20220817 00:00:00 to 20230202 00:00:00 UTC**<br>e) IW's attestation (See Appendix C on page 46).<br>f) SA's attestation (See Appendix D on page 47 and Appendix E on page 48).<br><br>All TEBs are labeled **Root DNSSEC KSK Ceremony 48**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage. | JD | +1<br>18:13 |

# 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 -xvf 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 46.

## 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 47.

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

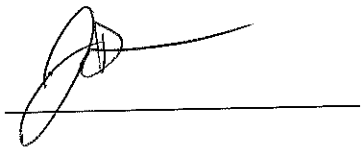
## 7. Other items

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: **Jonathan Denison**

Signature: 

Date: 2023 Feb 02

# 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:

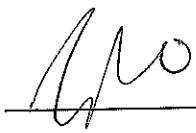
a) There were NO discrepancies found in the system configurations, assigned authorizations and audit logs.
b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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: **20220817 00:00:00 to 20230202 00:00:00 UTC.**

SA: Josh Jenkins

Signature: 

Date: 2023 Feb 2

# 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: Josh Jenkins

Signature:

Date: 2023 Feb 2

```
system {
    host-name srx;
    root-authentication {
        encrypted-password "XXXX"; ## SECRET-DATA
    }
    login {
        user bmartin {
            full-name "Brian Martin";
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user cbarthold {
            full-name "Connor A. Barthold";
            uid 2004;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user dkara {
            full-name "Darren Kara";
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user jjenkins {
            full-name "Josh Jenkins";
            uid 2007;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user mcirilo {
            full-name "Moises D. Cirilo";
            uid 2006;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user ptudor {
            full-name "Patrick Tudor";
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user rquinn {
            full-name "Reed Quinn";
            uid 2003;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        user sfreeark {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "XXXX"; ## SECRET-DATA
            }
        }
        password {
            format sha512;
        }
    }
    services {
        ssh {
            root-login deny;
        }
    }
    domain-name ksk.lax.dns.icann.org;
    location {
        country-code US;
        postal-code 90245;
        building Equinix-LA3;
        floor 1;
        rack 1;
    }
    ports {
        console {
```

```
            log-out-on-disconnect;
            type vt100;
        }
    }
    name-server {
        192.0.42.53;
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    ntp {
        server 129.6.15.28;
        server 129.6.15.29;
    }
}
chassis {
    config-button no-rescue no-clear;
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
security {
    pki {
        ca-profile root-ca {
            ca-identity "ICANN Root CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
            administrator {
                email-address "cbo-team@iana.org";
            }
        }
        ca-profile intermediate-ca {
            ca-identity "ICANN SSL CA";
            revocation-check {
                crl {
                    disable on-download-failure;
                }
            }
        }
    }
    ike {
        proposal ike-proposal-KMF {
            authentication-method rsa-signatures;
            dh-group group24;
            authentication-algorithm sha-256;
            encryption-algorithm aes-256-cbc;
        }
        policy ike-policy-KMF {
            proposals ike-proposal-KMF;
            certificate {
                local-certificate ksk-lax;
            }
        }
        gateway Gateway-to-KMF-East {
            ike-policy ike-policy-KMF;
            address 64.124.6.5;
            local-identity distinguished-name;
            remote-identity distinguished-name;
            external-interface ge-0/0/15;
            version v2-only;
        }
    }
    ipsec {
        proposal IPSecProposal {
            protocol esp;
            authentication-algorithm hmac-sha-256-128;
```

```
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 7200;
    }
    policy defaultPolicy {
        perfect-forward-secrecy {
            keys group5;
        }
        proposals IPSecProposal;
    }
    vpn vpn-to-KMF-East {
        bind-interface st0.1;
        ike {
            gateway Gateway-to-KMF-East;
            ipsec-policy defaultPolicy;
        }
        establish-tunnels immediately;
    }
}
screen {
    ids-option external-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
    }
}
nat {
    source {
        rule-set internal-to-external {
            from zone [ access guest wifi ];
            to zone untrust;
            rule source-nat-rule {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
policies {
    from-zone access to-zone untrust {
        policy allow-mail {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-dns {
            match {
                source-address [ ACC ACS EVM IMS ];
                destination-address [ icann-dns google-dns ];
                application [ junos-dns-udp junos-dns-tcp ];
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
        policy allow-simplex {
            match {
                source-address IDP;
```

```
            destination-address simplex;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
}
from-zone access to-zone video {
    policy access-to-video {
        match {
            source-address IMS;
            destination-address kmf_west_video;
            application junos-icmp-all;
        }
        then {
            permit;
        }
    }
}
from-zone access to-zone ipsec {
    policy allow-access-to-ipsec {
        match {
            source-address [ ACS ACC ];
            destination-address [ kmf_east_acs kmf_east_acc ];
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy allow-access-access {
        match {
            source-address kmf_west_access;
            destination-address kmf_east_access;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ipsec to-zone access {
    policy allow-ipsec-to-access {
        match {
            source-address [ kmf_east_acs kmf_east_acc ];
            destination-address [ ACS ACC ];
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application junos-icmp-ping;
        }
        then {
            permit;
        }
    }
    policy allow-access-access {
        match {
            source-address kmf_east_access;
            destination-address kmf_west_access;
            application any;
        }
```

```
        then {
            permit;
        }
    }
}
from-zone video to-zone ipsec {
    policy allow-video-to-ipsec {
        match {
            source-address VSS;
            destination-address kmf_east_vss;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_west_video;
            destination-address kmf_east_video;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone guest to-zone untrust {
    policy allow-guest-to-untrust {
        match {
            source-address kmf_west_guest;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone wifi to-zone untrust {
    policy allow-wifi-to-untrust {
        match {
            source-address kmf_west_wifi;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ipsec to-zone video {
    policy allow-ipsec-to-video {
        match {
            source-address kmf_east_vss;
            destination-address VSS;
            application any;
        }
        then {
            permit;
            log {
                session-close;
            }
        }
    }
    policy allow-icmp {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    policy allow-access-video {
        match {
            source-address kmf_east_video;
            destination-address kmf_west_video;
            application any;
        }
        then {
            permit;
        }
    }
```

```
    }
    from-zone access to-zone access {
        policy allow-access {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone video to-zone untrust {
        policy allow-mail {
            match {
                source-address VSS;
                destination-address icann;
                application junos-smtp;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
    }
    default-policy {
        deny-all;
    }
}
zones {
    security-zone access {
        address-book {
            address ACS 10.4.28.203/32;
            address ACC 10.4.28.202/32;
            address IDP 10.4.28.201/32;
            address EVM 10.4.28.200/32;
            address IMS 10.4.28.204/32;
            address E1 10.4.28.210/32;
            address E3 10.4.28.212/32;
            address E4 10.4.28.213/32;
            address kmf_west_access 10.4.28.192/26;
            address localnet 10.4.28.0/24;
            address-set iris-scanners {
                address E1;
                address E3;
                address E4;
            }
        }
        interfaces {
            irb.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        ntp;
                        ssh;
                    }
                }
            }
        }
    }
    security-zone untrust {
        address-book {
            address icann 192.0.32.0/20;
            address icann-dns 192.0.42.53/32;
            address googledns1 8.8.8.8/32;
            address googledns2 8.8.4.4/32;
            address simplex1 216.224.218.31/32;
            address simplex2 216.224.218.32/32;
            address simplex3 216.224.218.33/32;
            address simplex4 216.224.218.34/32;
            address-set google-dns {
                address googledns1;
                address googledns2;
            }
            address-set simplex {
                address simplex1;
                address simplex2;
                address simplex3;
                address simplex4;
            }
        }
        screen external-screen;
        interfaces {
            ge-0/0/15.0 {
                host-inbound-traffic {
```

```
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone video {
    address-book {
        address kmf_west_video 10.4.28.128/26;
        address VSS 10.4.28.150/32;
        address C1 10.4.28.151/32;
        address C2 10.4.28.152/32;
        address C3 10.4.28.153/32;
        address-set cameras {
            address C1;
            address C2;
            address C3;
        }
    }
    interfaces {
        irb.1 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone guest {
    address-book {
        address STR 10.4.28.20/32;
        address VCC 10.4.28.22/32;
        address kmf_west_guest 10.4.28.0/25;
    }
    interfaces {
        irb.2 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
}
security-zone ipsec {
    address-book {
        address kmf_east_access 10.4.29.192/26;
        address kmf_east_video 10.4.29.128/26;
        address kmf_east_acs 10.4.29.204/32;
        address kmf_east_acc 10.4.29.202/32;
        address kmf_east_idp 10.4.29.201/32;
        address kmf_east_evm 10.4.29.200/32;
        address kmf_east_ims 10.4.29.203/32;
        address kmf_east_E1 10.4.29.210/32;
        address kmf_east_E2 10.4.29.211/32;
        address kmf_east_E3 10.4.29.212/32;
        address kmf_east_E4 10.4.29.213/32;
        address kmf_east_vss 10.4.29.150/32;
        address kmf_east_C1 10.4.29.151/32;
        address kmf_east_C2 10.4.29.152/32;
        address kmf_east_C3 10.4.29.153/32;
    }
    interfaces {
        st0.1 {
            host-inbound-traffic {
                system-services {
                    ping;
                    ike;
                }
            }
        }
    }
}
security-zone wifi {
    address-book {
        address kmf_west_wifi 10.100.1.0/24;
    }
    interfaces {
        irb.3 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
        }
    }
```

```
        }
    }
}
interfaces {
    ge-0/0/6 {
        ether-options {
            802.3ad ae0;
        }
    }
    ge-0/0/7 {
        ether-options {
            802.3ad ae0;
        }
    }
    ge-0/0/15 {
        unit 0 {
            family inet {
                address 192.0.35.202/26;
            }
        }
    }
    ae0 {
        aggregated-ether-options {
            lacp {
                active;
            }
        }
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [ vlan-access vlan-guest vlan-video vlan-wifi ];
                }
            }
        }
    }
    irb {
        unit 0 {
            description "access vlan";
            family inet {
                address 10.4.28.193/26;
            }
        }
        unit 1 {
            description "video vlan";
            family inet {
                address 10.4.28.129/26;
            }
        }
        unit 2 {
            description "guest vlan";
            family inet {
                address 10.4.28.1/25;
            }
        }
        unit 3 {
            description "wifi vlan";
            family inet {
                address 10.100.1.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input route-engine-filter;
                }
            }
        }
    }
    st0 {
        unit 1 {
            description "IPSec KMF-West";
            family inet;
        }
    }
}
policy-options {
    prefix-list resolver-servers {
        apply-path "system name-server <*>";
    }
    prefix-list local-prefixes {
        10.4.28.0/24;
    }
    prefix-list ntp-servers {
        129.6.15.28/32;
        129.6.15.29/32;
```

```
    }
    prefix-list remote-ike-peers {
        apply-path "security ike gateway <*> address <*>";
    }
}
firewall {
    family inet {
        filter route-engine-filter {
            term deny-icmp-redirects {
                from {
                    protocol icmp;
                    icmp-type redirect;
                }
                then {
                    discard;
                }
            }
            term allow-icmp {
                from {
                    protocol icmp;
                    icmp-type [ echo-request echo-reply unreachable time-exceeded ];
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-traceroute {
                from {
                    protocol udp;
                    port 33434-33534;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-dns {
                from {
                    source-prefix-list {
                        resolver-servers;
                    }
                    protocol udp;
                    source-port domain;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-ntp {
                from {
                    source-prefix-list {
                        local-prefixes;
                        ntp-servers;
                    }
                    protocol udp;
                    port ntp;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-establish {
                from {
                    protocol tcp;
                    tcp-established;
                }
                then accept;
            }
            term allow-ipsec-esp {
                from {
                    source-prefix-list {
                        remote-ike-peers;
                    }
                    protocol esp;
                }
                then accept;
            }
            term allow-ipsec-udp {
                from {
                    source-prefix-list {
                        remote-ike-peers;
                    }
                    protocol udp;
                    port 500;
                }
```

```
                then accept;
            }
            term allow-ike-fragments {
                from {
                    source-prefix-list {
                        remote-ike-peers;
                    }
                    is-fragment;
                    protocol udp;
                }
                then {
                    policer small-bw-limit;
                    accept;
                }
            }
            term allow-ssh {
                from {
                    source-address {
                        10.4.29.193/32;
                    }
                    protocol tcp;
                    destination-port ssh;
                }
                then accept;
            }
            term LAST {
                then {
                    discard;
                }
            }
        }
    }
    policer small-bw-limit {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 15k;
        }
        then discard;
    }
}
vlans {
    vlan-access {
        vlan-id 10;
        l3-interface irb.0;
    }
    vlan-guest {
        vlan-id 12;
        l3-interface irb.2;
    }
    vlan-video {
        vlan-id 11;
        l3-interface irb.1;
    }
    vlan-wifi {
        vlan-id 13;
        l3-interface irb.3;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.0.35.201;
        route 10.4.29.0/24 next-hop st0.1;
        route 64.124.6.5/32 next-hop 192.0.35.201;
    }
}
```