

Root DNSSEC KSK Ceremony 44

Wednesday 16 February 2022

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)


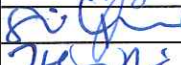



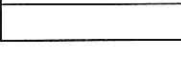

Abbreviations

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	Gustavo Lozano / ICANN		2022 Feb 17	01:27
IW	Jonathan Denison / ICANN			
SSC1	Sabrina Tanamal / PTI			
SSC2	Hilary Jin / ICANN			
SA	Josh Jenkins / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			

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

Instructions for a Root DNSSEC KSK Ceremony

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

Ceremony Guidelines:

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

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

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

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

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

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.	JD	21:00
2	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room), then performs a roll call using the list of participants on page 2.	JD	21:01
3	CA asks that any first time ceremony participants in the room introduce themselves.	JD	21:01
4	CA confirms that additional required personnel including COs, RZM, and Auditors are connected to the remote call. Scheduled remote participants are: CO4: Carlos Martinez (Key scripted for use) CO5: Olafur Gudmundsson (Key scripted for use) CO6: Nicolas Antonello (Key scripted for use) CO3: Joao Damas (Key designated as backup) RZM: Duane Wessels / Verisign RZM: Trevor Davis / Verisign AUD: Elvin Paik / RSM	JD	21:06

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
5	CA reviews emergency evacuation procedures with onsite participants.	JD	21:17
6	CA explains the use of personal electronic devices during the ceremony.	JD	21:17
7	CA summarizes the purpose of the ceremony.	JD	21:18

Verify the Time and Date

Step	Activity	Initials	Time
8	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: <u>2022-02-16 21:19:11</u> Note: All entries into this script or any logs should follow this common source of time.	JD	21:19

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: <u>1</u> Step(s): <u>9</u> Page(s): <u>6</u> Date and Time: <u>2022-02-16 21:25</u>	JD	21:25
2	IW describes the exception(s) and action(s) below.	JD	21:31

UPON INSPECTION OF SHIPPING ENVELOPE FOR CO4, IT APPEARS US CUSTOMS AND BORDER PATROL OPENED THE SHIPPING ENVELOPE AND RESEALED THE ENVELOPE WITH A YELLOW ADVISORY TAPE. INSIDE THE ENVELOPE, IT APPEARS US CUSTOMS CUT OPEN THE TEB LABELED BB91951317 AND FURCHER CUT OPEN THE INTERIOR ENVELOPE CONTAINING THE CO TENANT KEY. AS IT IS CLEAR THE TEB IS TAMPERED WITH, WE WILL PROCEED TO USE THE TENANT KEY ONE LAST TIME AND SUPPLY THE CO4 WITH A NEW KEY FOLLOWING THE CEREMONY, INCLUDING NEW SAFE DEPOSIT BOX.

NEW DEPOSIT BOX # 1791

ONE KEY WILL BE SHIPPED FIRST. ONCE RECEIPT IS CONFIRMED, SECOND KEY WILL BE DELIVERED AS WELL.

ACT 7 STEP 38

THERE WILL BE TWO TEBs FOR CO4 AS A RESULT OF HAVING TO SHIP KEYS SEPARATELY:

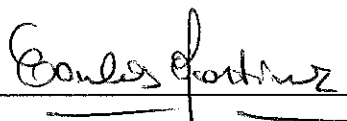
1 OF 2 BB91951251
2 OF 2 BB46584697

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Carlos Martinez am hereby entrusting my safe deposit box key enclosed in TEB # B391951317 for safe deposit box #1068 located within Safe #2 at the key management facility in El Segundo, CA.

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

Printed Name CARLOS MARTINEZ

Signature 

Date 1/26/2022

BB91951315

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Olafur Gudmundsson am hereby entrusting my safe deposit box key enclosed in TEB # BB 919 513 15 for safe deposit box #1789 located within Safe #2 at the key management facility in El Segundo, CA.

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

Printed Name OLAFUR GUDMUNDSSON

Signature 

Date 2024/1/26

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Nicolas Antoniello am hereby entrusting my safe deposit box key enclosed in TEB # BB91951313 for safe deposit box #1073 located within Safe #2 at the key management facility in El Segundo, CA.

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

Printed Name

Nicolas Antoniello

Signature



Date

25 / Jan / 2022

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I Joao Luis Silva Damas am hereby entrusting my safe deposit box key enclosed in TEB # 0891951319 for safe deposit box #1069 located within Safe #2 at the key management facility in El Segundo, CA.

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

Printed Name JOAO LUIS SILVA DAMAS

Signature J. L. Damas

Date 26 / JAN / 2022

Crypto Officer Key Verification

Step	Activity	Initials	Time
9	<p>The CA performs the following steps to verify the listed CO keys:</p> <ol style="list-style-type: none"> Remove the TEB from the shipping envelope and discard the shipping envelope. Inspect the TEB for tamper evidence. Read aloud the TEB number and place the TEB on the ceremony table visible to the audit camera. Open the TEB and place its contents on the ceremony table. Give the CO key declaration to IW to verify the CO key TEB number then insert the declaration into the audit bundle. Discard the TEB. Remove the CO tenant key from the padded envelope, and set the envelope aside for return shipping post-ceremony. Give the CO tenant key to the IW. <p>CO4: Carlos Martinez Key TEB # BB91951317 (See Appendix F on page 47)</p> <p>CO5: Olafur Gudmundsson Key TEB # BB91951315 (See Appendix G on page 48)</p> <p>CO6: Nicolas Antonello Key TEB # BB91951313 (See Appendix H on page 49)</p> <p>Note 1: The CO3 Joao Damas Safe Deposit Box Key TEB # BB91951319 has been designated as a backup. See Appendix I on page 50. Note 2: The COs' tenant keys were individually transmitted to separate trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.</p>	JD	21:37

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
10	CA transport the guard key, a flashlight, and with IW escort SSC2 into Tier 5 (Safe Room.)	JD	21:38
11	SSC2 opens Safe #2 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.	JD	21:40
12	<p>Perform the following steps to complete the safe log:</p> <ol style="list-style-type: none"> SSC2 removes the existing safe log, then shows the most recent page to the audit camera. IW provides the pre-printed safe log to SSC2. SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies the entry then initials it. 	JD	21:41

Extract CO Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
13	<p>IW performs the following steps sequentially to retrieve the required TEBs:</p> <p>a) IW announces the name of the CO whose credentials will be extracted and requests their authorization to open their assigned safe deposit box.</p> <p>b) After the CO provides authorization, the CA operates the guard key in the bottom lock, then the IW uses the CO's tenant key to operate the top lock and opens their assigned safe deposit box.</p> <p>c) IW reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB.</p> <p>d) IW reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above.</p> <p>e) IW retains the TEB(s) specified below, returns any TEBs not required, then closes and locks the safe deposit box with assistance from the CA.</p> <p>f) IW writes the date and time, then signs the safe log where "Remove" is indicated.</p> <p>g) CA verifies the completed safe log entries, then initials it.</p> <p>CO4: Carlos Martinez Box # 1068 OP TEB # BB91951297 (Retain) SO TEB # BB46584665 (Retain)</p> <p>CO5: Olafur Gudmundsson Box # 1789 OP TEB # BB91951296 (Retain) SO TEB # BB46584381 (Retain)</p> <p>CO6: Nicolas Antonello Box # 1073 OP TEB # BB91951295 (Retain) SO TEB # BB46584383 (Retain)</p>	JD	21:55

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
14	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the entry then initials it.	JD	21:56
15	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	JD	21:57
16	CA, IW, and SSC2 leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	JD	21:57
17	IW places the TEBs on the ceremony table.	JD	21:58

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
18	CA and IW transport a cart, and escort SSC1 into Tier 5 (Safe Room.)	JD	21:59
19	SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.	JD	22:01
20	Perform the following steps to complete the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.	JD	22:02

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

Step	Activity	Initials	Time
21	<p>CA performs the following steps to extract each piece of equipment from the safe:</p> <p>a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified in the list below. d) Write the date, time, and signature on the safe log where "Remove" is indicated. e) IW verifies the safe log entry, then initials it.</p> <p>HSM3: TEB # BB51184234 (Check and Return) <i>Last Verified: AC Ceremony 40-4 2020-02-16</i></p> <p>HSM4: TEB # BB51184285 (Check and Return) <i>Last Verified: KSK Ceremony 42 2021-02-11</i></p> <p>HSM5W: TEB # BB51184239 (Place on Cart) <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>HSM6W: TEB # BB51184287 (Place on Cart) <i>Last Verified: AT Ceremony 44 2022-02-15</i></p> <p>Laptop3: TEB # BB81420121 (Place on Cart) <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>Laptop4: TEB # BB81420089 (Check and Return) <i>Last Verified: KSK Ceremony 42 2021-02-11</i></p> <p>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951322 (Place on Cart) <i>Last Verified: KSK Ceremony 42 2021-02-11</i></p> <p>KSK-2017: TEB # BB46584387 (Place on Cart) <i>Last Verified: KSK Ceremony 38 2019-08-14</i></p> <p>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>	JD	22:09

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

Step	Activity	Initials	Time
22	SSC1 writes the date and time, then signs the safe log where " Close Safe " is indicated. IW verifies the safe log entry then initials it.	JD	22:09
23	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	22:10
24	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	JD	22:10

Act 2: Equipment Setup

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

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

Laptop Setup

Step	Activity	Initials	Time
1	<p>CA performs the following steps to prepare the listed equipment:</p> <ul style="list-style-type: none"> a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. <p>HSM5W: TEB # BB51184239 / Serial # H1903017 <i>Last Verified: KSK Ceremony 41 2020-04-23</i> Laptop3: TEB # BB81420121 / Service Tag # C8SVSG2 <i>Last Verified: KSK Ceremony 41 2020-04-23</i> OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951322 <i>Last Verified: KSK Ceremony 42 2021-02-11</i></p> <p>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>	JD	22:16
2	<p>CA performs the following steps to confirm that no hard drive and battery are in the laptop:</p> <ul style="list-style-type: none"> a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty. 	JD	22:16
3	<p>CA performs the following steps to boot the laptop:</p> <ul style="list-style-type: none"> a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into the serial port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Immediately insert the OS DVD release coen-0.4.0 after the laptop power is switched ON. 	JD	22:18
4	<p>CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the View menu and select Zoom In or Zoom Out To change the resolution of each screen: Go to Applications > Settings > Display</p>	JD	22:20

February 15, 2022



To Whom It May Concern:

This is a letter of Verification of Employment for Trevor Davis. VeriSign, Inc. ("Verisign") has employed Trevor Davis full-time since September 29, 2014, currently as a Manager – Product Operations in Verisign's Production Operations department.


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

For more than 24 years, Verisign has maintained 100 percent operational accuracy and stability for .com and .net-managing and protecting the DNS infrastructure for over 163.7 million .com and .net domain names and processing more than 219 billion query transactions daily-keeping the world connected online, seamlessly and securely. Verisign is experienced in and provides support for both IPv6 and [DNSSEC](#).

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

Sincerely,

2/15/2022

X 

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

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



VERISIGN™

16 February 2022

The SHA256 hash of the KSR file ksr-root-2022-q2-0.xml
is:

**9a9ffc75b62c6fc085778080264e7171f4c1843205eee1ebf8694d754
c9fc79d**

The PGP word list for the hash above is:

**pupil opulent wayside impartial Scotland Chicago gremlin
recipe music inception merit intention bookshelf
distortion hamlet hideaway upshot recover mural component
adult universe tempest underfoot Vulcan guitarist
dreadful impartial drainage opulent soybean Ohio**

Attested on behalf of Verisign by:

Trevor Davis
Manager
Product Operations
Verisign, Inc.

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

OS DVD Checksum Verification

Step	Activity	Initials	Time
5	<p>CA uses the terminal window to executes the following steps:</p> <p>a) Calculate the SHA-256 hash by executing: <code>sha2wordlist < /dev/sr0</code></p> <p>b) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.</p> <p>Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.</p> <p>SHA-256 hash: 8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f</p> <p>PGP Words: minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document</p> <p>Note: The SHA-256 hash of the OS DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/44</p>	JD	22:22

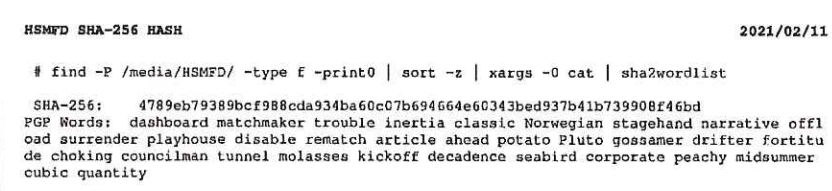
Printer Setup

Step	Activity	Initials	Time
6	<p>CA confirms that the printer is switched ON, then executes the command below using the terminal window to configure the printer and print a test page: <code>configure-printer</code></p>	JD	22:23

Date Setup

Step	Activity	Initials	Time
7	<p>CA executes <code>date</code> using the terminal window to verify if the date/time reasonably matches the ceremony clock.</p> <p>If the date/time do not match, perform the following steps:</p> <p>a) Execute <code>date -s "20220216 HH:MM:00"</code> to set the time. where HH is two-digit hour, MM is two-digit minutes and 00 is zero seconds.</p> <p>b) Execute <code>date</code> to confirm the date/time matches the clock.</p>	JD	22:24

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the Ceremony 42 HSMFD into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window.	JD	22:25
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: <code>hsmfd-hash -c</code> CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script.  IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 42 annotated script.	JD	22:26

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused HSMFD 42 and the sheet of paper with the printed HSMFD hash to RKOS.	JD	22:27

Start the Terminal Session Logging

Step	Activity	Initials	Time
11	CA executes the command below using the terminal window to change the working directory to HSMFD: <code>cd /media/HSMFD</code>	JD	22:27
12	CA executes the command below to log activities of the Commands terminal window: <code>script script-20220216.log</code>	JD	22:28

Start the HSM Activity Logging

Step	Activity	Initials	Time
13	CA performs the following steps using the HSM Output terminal window to capture the activity logs of the HSM: a) Change the working directory to HSMFD by executing: <code>cd /media/HSMFD</code> b) Set the serial port baud rate by executing: <code>stty -F /dev/ttyS0 115200</code> c) Start logging the serial output by executing: <code>ttyaudit /dev/ttyS0</code> Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the serial port.	JD	22:29

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none"> a) Verify the label on the HSM reads HSM5W b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. <p>Note: Status information should appear on the HSM activity logging screen.</p> <ul style="list-style-type: none"> d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads H1903017, then scroll back to the bottom. <p>HSM5W: Serial # H1903017</p> <p>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</p>	JD	22:30

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

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

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

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
1	<p>CA performs the following steps to verify the COs' credentials:</p> <p>a) Read aloud the TEB number, then inspect it for tamper evidence.</p> <p>b) Open the TEB, then remove the plastic case containing the card(s).</p> <p>c) Open the plastic case, then place the enclosed card(s) on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table.</p> <p>CO4: Carlos Martinez OP TEB # BB91951297 SO TEB # BB46584665</p> <p>CO5: Olafur Gudmundsson OP TEB # BB91951296 SO TEB # BB46584381</p> <p>CO6: Nicolas Antonello OP TEB # BB91951295 SO TEB # BB46584383</p>	JD	22:35

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
2	<p>CA performs the following steps to activate the HSM:</p> <p>a) Utilize the HSM's keyboard to scroll through the menu using < ></p> <p>b) Select "1.Set Online", press ENT to confirm.</p> <p>c) When "Set Online?" is displayed, press ENT to confirm.</p> <p>d) When "Insert Card OP #X?" is displayed, insert the OP card.</p> <p>e) When "PIN?" is displayed, enter "11223344", then press ENT.</p> <p>f) When "Remove Card?" is displayed, remove the OP card.</p> <p>g) Repeat steps d) to f) for the 2nd and 3rd OP cards.</p> <p>Confirm the "READY" LED on the HSM is ON. IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>1st OP card <u>4</u> of 7 2nd OP card <u>5</u> of 7 3rd OP card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	22:40

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
3	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	JD	22:40
4	CA performs the following steps to test the network connectivity between laptop and HSM: a) Use the Commands terminal window b) Test connectivity by executing: <code>ping hsm</code> c) Wait for responses, then exit by pressing: <code>Ctrl + C</code>	JD	22:41

Insert the KSRFD

Step	Activity	Initials	Time
5	CA plugs the FD labeled " KSR " into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window. Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.	JD	22:42

Execute the KSR Signer for KSR 2022 Q2

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: <code>ksrsigner /media/KSR/KSK44/ksr-root-2022-q2-0.xml</code>	JD	22:42
7	When the KSR signer displays the prompt: Activate HSM prior to accepting in the affirmative!! (y/N) : CA confirms that the HSM is online, then enters "y" to proceed.	JD	22:43

Verify the KSR Hash for KSR 2022 Q2

Step	Activity	Initials	Time
8	<p>When the hash of the KSR is displayed in the terminal window, perform the following:</p> <p>a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification off camera for the purpose of authentication while maintaining privacy.</p> <p>Note: If the RZM representative is not physically present in the room, write the representative's name and "<i>Remote Participant</i>" next to the name on the signature line.</p> <p>b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line:</p> <p>Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS in advance to be included in the final annotated script and audit bundle.</p> <p><u>TREVOR LEWIS DAVIS (REMOTE PARTICIPANT)</u></p> <p>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.</p>	JD	22:49
9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks " are there any objections? "	JD	22:49
10	CA enters " y " in response to " Is this correct (y/N)? " to complete the KSR signing operation. The SKR is located in: <code>/media/KSR/KSK44/skr-root-2022-q2-0.xml</code>	JD	22:49

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
11	<p>CA executes the commands below using the terminal window to print the KSR Signer log:</p> <p>a) <code>lpadmin -p HP -o copies-default=X</code> Note: Replace "X" with the amount of copies needed for the participants.</p> <p>b) <code>printlog ksrsigner-202202*.log</code></p>	JD	22:50
12	IW attaches a copy of the required ksrsigner log to their script.	JD	22:51

Starting: ksrsigner /media/KSR/KSK44/ksr-root-2022-q2-0.xml (at Wed Feb 16 22:42:54 2022 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0

HSM Information:
Label: ICANNKSK
ManufacturerID: Ultra Electronics AEP Networks
Model: Keyper 9860-2
Serial: H1903017

Validating last SKR with HSM...

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

Validate and Process KSR /media/KSR/KSK44/ksr-root-2022-q2-0.xml...

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

SHA256 hash of KSR:
9A9FFC75B62C6FC085778080264E7171F4C1843205EEE1EBF8694D754C9FC79D
>> pupil opulent wayside impartial Scotland Chicago gremlin recipe music inception merit intention bookshelf distortion h
amlet hideaway upshot recover mural component adult universe tempest underfoot Vulcan guitarist dreadful impartial draina
ge opulent soybean Ohio <<

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

- # KSK Tag (CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S

Generated new SKR in /media/KSR/KSK44/skr-root-2022-q2-0.xml

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

SHA256 hash of SKR:
EC50BDC13BA23719F13FBEEB755C3F0AB43A5672528870C78C9F395BF00958B6
>> tumor embezzle skullcap recover clockwork Pacific clamshell bottomless unwind customer skydive underfoot indulge fasci
nate cowbell Apollo scenic corrosion egghead holiness Dupont maritime guidance retraction offload opulent classroom exodu
s unearth applicant endorse potato <<
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
13	<p>CA executes the following commands using the terminal window:</p> <p>a) List the contents of the KSRFD by executing: <code>ls -ltrR /media/KSR</code></p> <p>b) Copy the contents of the KSRFD to the HSMFD by executing: <code>cp -pR /media/KSR/* .</code></p> <p>Note: Confirm overwrite by entering "y" if prompted.</p> <p>c) List the contents of the HSMFD to verify it has been copied successfully by executing: <code>ls -ltrR</code></p> <p>d) Unmount the KSRFD by executing: <code>umount /media/KSR</code></p>	JD	22:53
14	<p>CA removes the KSRFD containing the SKR files, then gives it to the RZM representative.</p> <p>Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.</p>	JD	22:53

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
15	<p>CA deactivates the HSM by performing the following steps:</p> <p>Note: CA will use OP cards not previously utilized in this ceremony if available.</p> <p>a) CA displays the HSM activity logging terminal window</p> <p>b) Utilize the HSM's keyboard to scroll through the menu using <></p> <p>c) Select "2.Set Offline", press ENT to confirm.</p> <p>d) When "Set Offline?" is displayed, press ENT to confirm.</p> <p>e) When "Insert Card OP #X?" is displayed, insert the OP card from the card holder.</p> <p>f) When "PIN?" is displayed, enter "11223344", then press ENT.</p> <p>g) When "Remove Card?" is displayed, remove the OP card.</p> <p>h) Repeat steps e) to g) for the 2nd and 3rd OP cards.</p> <p>Confirm the "READY" LED on the HSM is OFF. IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>1st OP card <u>4</u> of 7 2nd OP card <u>5</u> of 7 3rd OP card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	22:56

Act 4: RKSH SMK Credential Verification

To ensure the integrity and functionality of RKSH SMK credentials, inspection and testing will be performed.

The CA will test the credentials and transfer them to new tamper evident packaging by performing the steps below:

Verify SMK Readability

Step	Activity	Initials	Time
1	<p>CA perform the following steps:</p> <ul style="list-style-type: none"> a) Read aloud the SMK TEB number. b) Inspect the SMK TEB for tamper evidence. c) Open the TEB and place the SMK cards on the cardholder visible to everyone. <p>RKSH7: Kim Davies (Interim Custodian) SMK TEB # BB91951364 (Wrapped) - A14377110 (Original)</p>	JD	22:58
2	CA selects the HSM Output terminal window.	JD	22:59
3	<p>CA verifies that the SMK cards are readable by following the steps below:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using <> b) Select "8.View Cards", press ENT to confirm. c) When "View Cards?" is displayed, press ENT to confirm. d) When "Insert Card?" is displayed, insert the SMK card. e) Verify that SMK is displayed on the HSM, then press ENT four times to display the information on the terminal window. f) When "Remove Card?" is displayed, remove the SMK card. g) When "Another Card?" is displayed, press ENT to confirm. h) When "Insert Card?" is displayed, insert the next SMK card. i) Repeat steps e) to f) for the 2nd SMK card. j) Press CLR to return to the main menu "Secured". <p>IW records which cards were used below. The card is returned to card holder after use. SMK card <u>7</u> of 7 / Set <u>1</u> of 2 SMK card <u>7</u> of 7 / Set <u>2</u> of 2 Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	23:00

Place SMK into TEB

Step	Activity	Initials	Time
4	<p>CA perform the following steps:</p> <ul style="list-style-type: none"> a) Gather the prepared SMK TEB and plastic case for the RKSH credentials. b) Place the SMK cards in the plastic case. c) Place the plastic case into the TEB, read aloud the TEB number and description, then seal it. d) CA and IW inspect the TEB, then initial it with a ballpoint pen. IW keeps the sealing strips for later inventory. e) CA gives the TEB to RKOS to courier back to the interim custodian after the ceremony. <p>RKSH7: Kim Davies (Interim Custodian) SMK TEB # BB91951260</p>	JD	23:03

Act 5: Issue Temporary CO, AAK, and SMK Cards

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

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

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

Issue Temporary Crypto Officer (CO) Cards

Step	Activity	Initials	Time
1	CA selects the HSM Output terminal window.	JD	23:04
2	<p>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:</p> <p>a) Utilize the HSM's keyboard to scroll through the menu using < ></p> <p>b) Select "7.Role Mgmt", press ENT to confirm.</p> <p>c) When "Insert Card SO #X?" is displayed, insert the SO card.</p> <p>d) When "PIN?" is displayed, enter "11223344", then press ENT.</p> <p>e) When "Remove Card?" is displayed, remove the SO card.</p> <p>f) Repeat steps c) to e) for the 2nd and 3rd SO card.</p> <p>g) Select "1.Issue Cards", press ENT to confirm.</p> <p>h) Select "1.Issue CO Cards", press ENT to confirm.</p> <p>i) When "Issue CO Cards?" is displayed, press ENT to confirm.</p> <p>j) When "Num Cards?" is displayed, enter "2", then press ENT.</p> <p>k) When "Num Req Cards?" is displayed, enter "2", then press ENT.</p> <p>l) When "Insert Card #X?" is displayed, insert the required CO card.</p> <p>m) When "Remove Card?" is displayed, remove the CO card.</p> <p>n) Repeat steps l) to m) for the 2nd CO card.</p> <p>o) When "CO Cards Issued" is displayed, press ENT to confirm.</p> <p>p) Press CLR to return to the menu "Role Mgmt".</p> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # <u>1</u></p> <p>1st SO card <u>4</u> of 7</p> <p>2nd SO card <u>5</u> of 7</p> <p>3rd SO card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p> <p>Note: The default PIN for a new card is set as 11223344.</p>	JD	23:08

Issue Temporary Adapter Authorization Key (AAK) Cards

Step	Activity	Initials	Time
3	<p>CA performs the following steps to issue Adapter Authorization Key (AAK) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "3.Backup AAK" from the same menu "Role Mgmt", press ENT to confirm. c) When "Backup AAK?" is displayed, press ENT to confirm. d) When "Num Cards?" is displayed, enter "2", then press ENT. e) When "Insert Card #X?" is displayed, insert the required AAK card. f) When "Remove Card?" is displayed, remove the AAK card. g) Repeat steps e) to f) for the 2nd AAK card. h) When "Done AAK" is displayed, press ENT to confirm. i) Press CLR to return to the menu "Secured". <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	23:10

Issue Temporary Storage Master Key (SMK) Cards

Step	Activity	Initials	Time
4	<p>CA performs the following steps to issue Storage Master Key (SMK) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "5.Key Mgmt", press ENT to confirm. c) When "Insert CO Card #X?" is displayed, insert the CO card. d) When "PIN?" is displayed, enter "11223344", then press ENT. e) When "Remove Card?" is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select "4.SMK", press ENT to confirm. h) Select "2.Backup SMK", press ENT to confirm. i) When "Backup SMK?" is displayed, press ENT to confirm. j) When "Num Cards?" is displayed, enter "4", then press ENT. k) When "Num Req Cards?" is displayed, enter "2", then press ENT. l) When "Insert Card #X?" is displayed, insert the required SMK card. m) When "Remove Card?" is displayed, remove the SMK card. n) Repeat steps l) to m) for the 2nd, 3rd and 4th SMK cards. o) When "Verify Card #X?" is displayed, insert the required SMK card. p) When "Remove Card?" is displayed, remove the SMK card. q) Repeat steps o) to p) for the 2nd, 3rd and 4th SMK cards. r) When "SMK Backed Up" is displayed, press ENT to confirm. s) Press CLR twice to return to the main menu "Secured". <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	23:16

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
5	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. Note: DO NOT unplug the cable connections on the laptop.	JD	23:17
6	CA places the HSM into a prepared TEB, then seals it.	JD	23:19
7	CA performs the following steps: a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM TEB on the cart. HSM5W: TEB # BB51184290 / Serial # H1903017	JD	23:19

Act 6: Introduce New HSM

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

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

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
1	<p>CA performs the following steps to prepare the new HSM:</p> <ol style="list-style-type: none"> Remove the TEB from the cart and place it on the ceremony table. Inspect the TEB for tamper evidence. Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. Plug the null modem cable into the serial port of the HSM. Connect the power to the HSM, then switch it ON. <p>Note: Status information should appear on the HSM activity logging screen.</p> <ol style="list-style-type: none"> Scroll the logging screen up and locate the HSM serial number. IW verifies the displayed HSM serial number on the screen with the information below, then the CA scrolls back to the bottom. After the completion of the HSM self test the display should say "Important Read Manual" indicating the HSM is in the initialized state. <p>HSM6W: TEB # BB51184287 / Serial # H2008009 Last Verified: AT Ceremony 44 2022-02-15</p> <p>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</p> <p>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>	JO	23:22

Import the AAK

Step	Activity	Initials	Time
2	<p>CA performs the following steps to import the Adapter Authorization Key (AAK):</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using <> Select "2.Restore AAK", press ENT to confirm. When "Restore AAK?" is displayed, press ENT to confirm. When "Insert Card #X?" is displayed, insert the required AAK card and press ENT. When "Remove Card?" is displayed, remove the AAK card. Repeat steps d) to e) for the 2nd AAK card. When "Done AAK Imported" is displayed, press ENT to confirm. <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JO	23:24

Configure the HSM to Secure State

Step	Activity	Initials	Time
3	<p>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:</p> <ol style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "3.Secure", press ENT to confirm. c) When "Secure?" is displayed, press ENT to confirm. d) When "Insert Card SO #X?" is displayed, insert the SO card. e) When "PIN?" is displayed, enter "11223344", then press ENT. f) When "Remove Card?" is displayed, remove the SO card. g) Repeat steps d) to f) for the 2nd and 3rd SO cards. h) When "SMK AES Triple DES?" is displayed, press CLR to skip. i) When "SMK AES" is displayed, press ENT to confirm. j) When "LAN Port Number?" is displayed, press CLR to skip. k) When "Enable IPv4/IPv6?" is displayed, press CLR to skip. l) When "LAN IPv4 Address?" is displayed, press CLR to skip. m) When "LAN IPv4 Mask?" is displayed, press CLR to skip. n) When "Set IPv4 Gateway?" is displayed, press CLR to skip. o) When "LAN IPv6 Address?" is displayed, press CLR to skip. p) When "LAN IPv6 Mask?" is displayed, press CLR to skip. q) When "Set IPv6 Gateway?" is displayed, press CLR to skip. r) When "Remote Mgmt Off Enable?" is displayed, press CLR to skip. s) When "Remote Mgmt Off" is displayed, press ENT to confirm. t) When "Change Clock?" is displayed, press CLR to skip. u) When "Import Config?" is displayed, press CLR to skip. v) When "FIPS Mode On Disable?" is displayed, press CLR to skip. w) When "FIPS Mode On" is displayed, press ENT to confirm. x) When "Global Key Export Enabled" is displayed, press CLR to skip. <p>Done Rebooting Device will be displayed. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # <u>2</u> 1st SO card <u>4</u> of 7 2nd SO card <u>5</u> of 7 3rd SO card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	<p style="text-align: center;">JD</p>	<p style="text-align: center;">23:28</p>

Change the API Settings

Step	Activity	Initials	Time
4	<p>CA performs the following steps to change the API settings:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "5.Key Mgmt", press ENT to confirm. c) When "Insert CO Card #X?" is displayed, insert the CO card. d) When "PIN?" is displayed, enter "11223344", then press ENT. e) When "Remove Card?" is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select "5. API Settings", press ENT to confirm. h) Select "1.Key Import", press ENT to confirm. i) When "Key Import On Disable?" is displayed, press ENT to confirm. j) Select "2.Key Export", press ENT to confirm. k) When "Key Export On Disable?" is displayed, press ENT to confirm. l) Select "5.Sym Key Der", press ENT to confirm. m) When "Sym Key Der On Disable?" is displayed, press ENT to confirm. n) Press CLR twice to return to the main menu "Secured". <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	<p>JB</p>	<p>23:30</p>

Verify API Settings

Step	Activity	Initials	Time
5	<p>CA performs the following steps to dump the status of the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using <> Select "4.HSM Info", press ENT to confirm. Select "8.Output Info", press ENT to confirm. When "Output Info?" is displayed, press ENT to confirm. Press CLR to return to the main menu "Secured". <p>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:</p> <pre> Modes: (1=Enabled 0=Disabled) Global Key Export 1 App Key Import 0 App Key Export 0 Asymmetric Key Gen 1 Symmetric Key Gen 1 Symmetric Key Derive 0 Signing 1 Signature Verify 1 MAC Generation 1 MAC Verification 1 Encrypt / Decrypt 1 Delete Asym Key 1 Delete Sym Key 1 Output Key Details 1 Output Key Summary 1 Suite B Algorithms 1 Non Suite B Algs 1 Auto Online 0 Remote Management 0 AES SMK Set Offline FIPS Mode </pre>	JD	23:32

App Key Backups

Step	Activity	Initials	Time
6	<p>CA performs the following steps to prepare the App key backups:</p> <ol style="list-style-type: none"> Remove the TEB from the cart and place it on the ceremony table. Inspect the TEB for tamper evidence. Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. Remove and discard the TEB, then place the backup HSMFD on its designated area of the ceremony table. Using a sharpie, write 1 and 2 respectively on the App key cards, then place them on the designated card holder. <p>KSK-2017: TEB # BB46584387 Last Verified: KSK Ceremony 38 2019-08-14</p> <p>Note: <i>"Last verified"</i> indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>	JD	23:35

Import the SMK and the KSK

Step	Activity	Initials	Time
7	<p>CA performs the following steps to import Storage Master Key (SMK):</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using <> Select "5.Key Mgmt", press ENT to confirm. When "Insert CO Card #X?" is displayed, insert the CO card. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the CO card. Repeat steps c) to e) for the 2nd CO card. Select "4.SMK", press ENT to confirm. Select "3.Restore SMK", press ENT to confirm. When "Restore SMK?" is displayed, press ENT to confirm. When "Insert Card SMK #X?" is displayed, insert the SMK card. When "Remove Card?" is displayed, remove the SMK card. Repeat steps j) to k) for the 2nd SMK card. When "SMK Restored" is displayed, press ENT to confirm. Press CLR once to return to the main menu "Key Mgmt". <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	23:38
8	<p>CA performs the following steps to import KSK:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using <> Select "3.App Keys" from the current "Key Mgmt" menu, press ENT to confirm. Select "2.Restore", press ENT to confirm. When "Restore?" is displayed, press ENT to confirm. When "Which Media?" is displayed, select "2. From Card", press ENT to confirm. When "Insert Card #X?" is displayed, insert the required KSK card. When "Remove Card?" is displayed, remove the KSK card. When "Restore Complete" is displayed, press ENT to confirm. Press CLR twice to return to the main menu "Secured". <p>IW records which card was used below. Card is returned to its designated card holder after use. App Key card <u> 1 </u></p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	23:39

Return the KSK into a TEB

Step	Activity	Initials	Time
9	CA places the KSK and the backup HSMFD into a prepared TEB, then seals it.	JD	23:42
10	<p>CA performs the following steps:</p> <ol style="list-style-type: none"> Read aloud the TEB number, then show it to the audit camera above for participants to see. Confirm with IW that the TEB number matches below. Initial the TEB along with IW using a ballpoint pen. Give IW the sealing strips for post-ceremony inventory. Place the KSK TEB on the cart. <p>KSK-2017: TEB # BB91951258</p>	JD	23:42

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
11	<p>CA performs the following steps to activate the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "1.Set Online", press ENT to confirm. c) When "Set Online?" is displayed, press ENT to confirm. d) When "Insert Card OP #X?" is displayed, insert the OP card. e) When "PIN?" is displayed, enter "11223344", then press ENT. f) When "Remove Card?" is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. <p>Confirm the "READY" LED on the HSM is ON. IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>1st OP card <u>4</u> of 7 2nd OP card <u>5</u> of 7 3rd OP card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	23:44

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
12	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	JD	23:44
13	<p>CA performs the following steps to test the network connectivity between laptop and HSM:</p> <ul style="list-style-type: none"> a) Use the Commands terminal window b) Test connectivity by executing: <code>ping hsm</code> c) Wait for responses, then exit by pressing: <code>Ctrl + C</code> 	JD	23:45

Insert Copy of the KSRFD

Step	Activity	Initials	Time
14	<p>CA plugs the FD labeled "KSR_COPY" into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window.</p> <p>Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.</p>	JD	23:46

Execute the KSR Signer for KSR 2022 Q2

Step	Activity	Initials	Time
15	CA executes the command below in the terminal window to sign the KSR file: <code>ksrsigner /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml</code>	JD	23:47
16	<p>When the KSR signer displays the prompt: Activate HSM prior to accepting in the affirmative!! (y/N) : CA confirms that the HSM is online, then enters "y" to proceed.</p>	JD	23:47

Verify the KSR Hash for KSR 2022 Q2

Step	Activity	Initials	Time
17	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.	JD	23:48
18	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks " are there any objections? "	JD	23:48
19	CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in: /media/KSR_COPY/KSK44/skr-root-2022-q2-0.xml	JD	23:49

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
20	CA executes the commands below using the terminal window to print the KSR Signer log: a) <code>lpadmin -p HP -o copies-default=X</code> Note: Replace "X" with the amount of copies needed for the participants. b) <code>printlog \$(ls -tr ksrsigner-202202*.log tail -n 1)</code>	JD	23:50
21	IW attaches a copy of the required ksrsigner log to their script.	JD	23:50

Verification of the Hash of the SKR Copy

Step	Activity	Initials	Time
22	CA read the SHA256 hash in PGP wordlist format for the generated SKR and the ceremony participants match the hash with the previous SKR.	JD	23:51

Remove Copy of the KSRFD

Step	Activity	Initials	Time
23	CA executes the following commands using the terminal window: a) List the contents of the KSRFD by executing: <code>ls -ltrR /media/KSR_COPY</code> b) Unmount the KSRFD by executing: <code>umount /media/KSR_COPY</code>	JD	23:52
24	CA removes the KSR_COPY containing the SKR files, then gives it to IW for audit purpose.	JD	23:53

Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
25	CA selects the HSM Output terminal window and presses the RESTART button on the HSM to make it offline and waits for the self test to complete. Confirm the " READY " LED on the HSM is OFF .	JD	23:54

```

Starting: ksrsigner /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml (at Wed Feb 16 23:47:15 2022 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 2022-01-01T00:00:00 2022-01-22T00:00:00 09799,14748 20326(Klajeyz)/S
2 2022-01-11T00:00:00 2022-02-01T00:00:00 09799 20326(Klajeyz)/S
3 2022-01-21T00:00:00 2022-02-11T00:00:00 09799 20326(Klajeyz)/S
4 2022-01-31T00:00:00 2022-02-21T00:00:00 09799 20326(Klajeyz)/S
5 2022-02-10T00:00:00 2022-03-03T00:00:00 09799 20326(Klajeyz)/S
6 2022-02-20T00:00:00 2022-03-13T00:00:00 09799 20326(Klajeyz)/S
7 2022-03-02T00:00:00 2022-03-23T00:00:00 09799 20326(Klajeyz)/S
8 2022-03-12T00:00:00 2022-04-02T00:00:00 09799 20326(Klajeyz)/S
9 2022-03-22T00:00:00 2022-04-12T00:00:00 47671,09799 20326(Klajeyz)/S
...VALIDATED.

```

```

Validate and Process KSR /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-04-01T00:00:00 2022-04-22T00:00:00 47671,09799
2 2022-04-11T00:00:00 2022-05-02T00:00:00 47671
3 2022-04-21T00:00:00 2022-05-12T00:00:00 47671
4 2022-05-01T00:00:00 2022-05-22T00:00:00 47671
5 2022-05-11T00:00:00 2022-06-01T00:00:00 47671
6 2022-05-21T00:00:00 2022-06-11T00:00:00 47671
7 2022-05-31T00:00:00 2022-06-21T00:00:00 47671
8 2022-06-10T00:00:00 2022-07-01T00:00:00 47671
9 2022-06-20T00:00:00 2022-07-11T00:00:00 20826,47671
...PASSED.

```

```

SHA256 hash of KSR:
9A9FFC75B62C6FC085778080264E7171F4C1843205EEE1EBF8694D754C9FC79D
>> pupil opulent wayside impartial Scotland Chicago gremlin recipe music inception merit intention bookshelf distortion h
amlet hideaway upshot recover mural component adult universe tempest underfoot Vulcan guitarist dreadful impartial draina
ge opulent soybean Ohio <<

```

```

Reading KSK schedule "normal(2017)" from "kskschedule.json"
# KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S

```

```

Generated new SKR in /media/KSR_COPY/KSK44/skr-root-2022-q2-0.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-04-01T00:00:00 2022-04-22T00:00:00 47671,09799 20326(Klajeyz)/S
2 2022-04-11T00:00:00 2022-05-02T00:00:00 47671 20326(Klajeyz)/S
3 2022-04-21T00:00:00 2022-05-12T00:00:00 47671 20326(Klajeyz)/S
4 2022-05-01T00:00:00 2022-05-22T00:00:00 47671 20326(Klajeyz)/S
5 2022-05-11T00:00:00 2022-06-01T00:00:00 47671 20326(Klajeyz)/S
6 2022-05-21T00:00:00 2022-06-11T00:00:00 47671 20326(Klajeyz)/S
7 2022-05-31T00:00:00 2022-06-21T00:00:00 47671 20326(Klajeyz)/S
8 2022-06-10T00:00:00 2022-07-01T00:00:00 47671 20326(Klajeyz)/S
9 2022-06-20T00:00:00 2022-07-11T00:00:00 47671,20826 20326(Klajeyz)/S

```

```

SHA256 hash of SKR:
EC50BDC13BA23719F13FBEEB755C3F0AB43A5672528870C78C9F395BF00958B6
>> tumor embezzle skullcap recover clockwork Pacific clamshell bottomless unwind customer skydive underfoot indulge fasci
nate cowbell Apollo scenic corrosion egghead holiness Dupont maritime guidance retraction offload opulent classroom exodu
s unearth applicant endorse potato <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=0

```

Clear and Destroy SMK Cards

Step	Activity	Initials	Time
26	<p>CA performs the following steps to clear Storage Master Key (SMK) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "5.Key Mgmt", press ENT to confirm. When "Insert CO Card #X?" is displayed, insert the CO card. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the CO card. Repeat steps c) to e) for the 2nd CO card. Select "4.SMK", press ENT to confirm. Select "4.Clear Cards", press ENT to confirm. When "Clear Card?" is displayed, press ENT to confirm. When "Insert Card SMK 1?" is displayed, take the SMK #1 card from the cardholder, show the SMK #1 card to the audit camera and then insert the SMK #1 card into the HSM's card reader. When "Num Cards?" is displayed, enter "4", then press ENT. When "Are you sure?" is displayed, press ENT to confirm. When "Remove Card?" is displayed, remove the SMK card. When "Insert Card SMK #X?" is displayed, take the SMK #X card from the cardholder, show the SMK #X card to the audit camera and then insert the SMK #X card into the HSM's card reader. When "Are you sure?" is displayed, press ENT to confirm. When "Remove Card?" is displayed, remove the SMK card. Repeat steps n) to p) for the 3rd and 4th SMK cards. Press CLR twice to return to the main menu "Secured". CA uses the shredder to destroy the cleared SMK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder. <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	00:01

Clear and Destroy CO and AAK Cards

Step	Activity	Initials	Time
27	<p>CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to clear Crypto Officer (CO) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "7.Role Mgmt", press ENT to confirm. When "Insert Card SO #X?" is displayed, insert the SO card. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the SO card. Repeat steps c) to e) for the 2nd and 3rd SO card. Select "4.Clear RoleCard", press ENT to confirm. When "Clear Card?" is displayed, press ENT to confirm. When "Num Cards?" is displayed, enter "2", then press ENT. When "Insert Card #X?" is displayed, take the required CO #X card from the cardholder, show the CO #X card to the audit camera and then insert the CO #X card into the HSM's card reader. When "Are you sure?" is displayed, press ENT to confirm. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the CO card. Repeat steps j) to m) for the 2nd CO card. <p>IW records which cards were used below. Each card is returned to its designated card holder after use. Set # <u>1</u> 1st SO card <u>4</u> of 7 2nd SO card <u>5</u> of 7 3rd SO card <u>6</u> of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JA	00:05
28	<p>CA performs the following steps to clear Adapter Authorization Key (AAK) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "5.Clear AAK Card" from the same menu "Role Mgmt", press ENT to confirm. When "Clear AAK Card?" is displayed, press ENT to confirm. When "Num Cards?" is displayed, enter "2", then press ENT. 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. When "Are you sure?" is displayed, press ENT to confirm. When "Remove Card?" is displayed, remove the AAK card. Repeat steps e) to g) for the 2nd AAK card. Press CLR to return to the main menu "Secured". <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	JD	00:06
29	<p>CA uses the shredder to destroy the cleared CO and AAK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.</p>	JD	00:08

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
30	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. Note: DO NOT unplug the cable connections on the laptop.	JD	00:09
31	CA places the HSM into a prepared TEB, then seals it.	JD	00:10
32	CA performs the following steps: a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM TEB on the cart. HSM6W: TEB # BB51184288 / Serial # H2008009	JD	00:10

Act 7: Secure Hardware

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

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

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
1	CA performs the following steps to stop logging: a) Disconnect the null modem and ethernet cables from the laptop. b) Perform the following steps using the HSM Output terminal window to stop logging the serial output (ttyaudit): i) Press Ctrl + C ii) Execute exit c) Execute the command below using the Commands terminal window to stop logging the terminal session: exit Note: The Commands terminal session window will remain open.	JD	00:11

Prepare blank FDs and back up the HSMFD Contents

Step	Activity	Initials	Time
2	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: <code>shopt -s dotglob</code>	JD	00:12
3	CA executes the following commands using the terminal window to print 2 copies of the hash for the HSMFD content: a) <code>lpadmin -p HP -o copies-default=2</code> b) <code>hsmfd-hash -p</code> Note: One copy for audit bundle and one copy for HSMFD package.	JD	00:13
4	CA executes the command below using the terminal window to display the contents of the HSMFD: <code>ls -ltrR</code>	JD	00:14
5	CA executes the command below using the terminal window to create the mount point that will be used for the backup HSMFDs: <code>mkdir /media/HSMFD1</code>	JD	00:14
6	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it.	JD	00:15
7	CA closes the file system window, then executes the command below to verify the device name of the blank HSMFD: <code>df</code>	JD	00:15
8	CA executes the commands below to unmount, format, mount, and back up the HSMFD contents to the blank HSMFD: a) <code>umount /dev/sdc1</code> b) <code>mkfs.vfat -n HSMFD -I /dev/sdc1</code> c) <code>mount /dev/sdc1 /media/HSMFD1</code> d) <code>cp -pR * /media/HSMFD1</code>	JD	00:16
9	CA executes the commands below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy, then unmounts the flash drive before removal: a) <code>hsmfd-hash -m</code> b) <code>umount /media/HSMFD1</code>	JD	00:17
10	CA removes the HSMFD copy , then places it on the holder. Wait for the activity light on the backup HSMFD to stop flashing before removal.	JD	00:17
11	CA repeats step 6 to 10 for the 2 nd copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	JD	00:19
12	CA repeats step 6 to 10 for the 3 rd copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	JD	00:20
13	CA repeats step 6 to 10 for the 4 th copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	JD	00:21
14	CA repeats step 6 to 10 for the 5 th copy. Wait for the activity light on the backup HSMFD to stop flashing before executing each step.	JD	00:22

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

```
SHA-256: 19a74e4304c6e8ed65d81099a3e76e25b758c0cde58f99d5b157c3d906add5ac  
PGP Words: bedlamp paragraph drifter decimal adrift responsive trauma unify fracture stupe  
ndous assume nebula reform truncated goldfish caravan seabird everyday slowdown sandalwood  
topmost midsummer prowler specialist sailboat Eskimo snowcap supportive afflict perceptive  
sterling penetrate
```

Print Logging Information

Step	Activity	Initials	Time
15	<p>CA executes the following commands using the terminal window to print a copy of the logging information:</p> <p>a) <code>lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true</code></p> <p>b) <code>enscript -2Gr script-202202*.log</code></p> <p>c) <code>enscript -Gr --font="Courier8" ttyaudit-tty*-202202*.log</code></p> <p>Attach the printed copies to IW script. Note: Ignore the error regarding non-printable characters if prompted.</p>	JD	00:25

Place HSMFDs and OS DVDs into a TEB

Step	Activity	Initials	Time
16	<p>CA executes the following commands using the terminal window to unmount the HSMFD:</p> <p>a) <code>cd /tmp</code></p> <p>b) <code>umount /media/HSMFD</code></p> <p>CA removes the HSMFD, then places it on the holder.</p>	JD	00:25
17	<p>CA performs the following steps to switch OFF the laptop and remove the OS DVD:</p> <p>a) Remove the OS DVD from the laptop.</p> <p>b) Turn OFF the laptop by pressing the power button.</p> <p>c) Disconnect all connections from the laptop.</p>	JD	00:26
18	CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it.	JD	00:27
19	<p>CA performs the following steps to verify the TEB:</p> <p>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.</p> <p>b) Confirm with IW that the TEB number matches with the information below.</p> <p>c) Initial the TEB along with IW using a ballpoint pen.</p> <p>d) Give IW the sealing strips for post-ceremony inventory.</p> <p>e) Place the OS DVD TEB on the cart.</p> <p>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951259</p>	JD	00:28
20	CA distributes the remaining HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	JD	00:28

02/17/22
00:11:30

script-20220216.log

1

```
Script started on Wed Feb 16 22:28:07 2022
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=0.717 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.581 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.730 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.612 ms
64 bytes from hsm (192.168.0.2): icmp_seq=5 ttl=255 time=0.583 ms
^C
--- hsm ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4093ms
rtt min/avg/max/mdev = 0.581/0.644/0.730/0.071 ms
root@coen:/media/HSMFD# ksr signer /media/KSR/KSK44/ks\007r-root-2022-q2-0.xml
Starting: ksr signer /media/KSR/KSK44/ksr-root-2022-q2-0.xml (at Wed Feb 16 22:42:54 2022
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: H1903017
```

```
Validating last SKR with HSM...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-01-01T00:00:00 2022-01-22T00:00:00 09799,14748 20326(Klajeyz)/S
2 2022-01-11T00:00:00 2022-02-01T00:00:00 09799 20326(Klajeyz)/S
3 2022-01-21T00:00:00 2022-02-11T00:00:00 09799 20326(Klajeyz)/S
4 2022-01-31T00:00:00 2022-02-21T00:00:00 09799 20326(Klajeyz)/S
5 2022-02-10T00:00:00 2022-03-03T00:00:00 09799 20326(Klajeyz)/S
6 2022-02-20T00:00:00 2022-03-13T00:00:00 09799 20326(Klajeyz)/S
7 2022-03-02T00:00:00 2022-03-23T00:00:00 09799 20326(Klajeyz)/S
8 2022-03-12T00:00:00 2022-04-02T00:00:00 09799 20326(Klajeyz)/S
9 2022-03-22T00:00:00 2022-04-12T00:00:00 47671,09799 20326(Klajeyz)/S
...VALIDATED.
```

```
Validate and Process KSR /media/KSR/KSK44/ksr-root-2022-q2-0.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-04-01T00:00:00 2022-04-22T00:00:00 47671,09799
2 2022-04-11T00:00:00 2022-05-02T00:00:00 47671
3 2022-04-21T00:00:00 2022-05-12T00:00:00 47671
4 2022-05-01T00:00:00 2022-05-22T00:00:00 47671
5 2022-05-11T00:00:00 2022-06-01T00:00:00 47671
6 2022-05-21T00:00:00 2022-06-11T00:00:00 47671
7 2022-05-31T00:00:00 2022-06-21T00:00:00 47671
8 2022-06-10T00:00:00 2022-07-01T00:00:00 47671
9 2022-06-20T00:00:00 2022-07-11T00:00:00 20826,47671
...PASSED.
```

```
SHA256 hash of KSR:
9A9FFC75B62C6FC085778080264E7171F4C1843205EEE1EBF8694D754C9FC79D
>> pupil opulent wayside impartial Scotland Chieago gremlin recipe music inception merit
intention bookshelf distortion hamlet hideaway upshot recover mural component adult unive
rse tempest underfoot Vulcan guitarist dreadful impartial drainage opulent soybean Ohio <
<
```

```
Is this correct (y/N)? y
Reading KSK schedule "normal(2017)" from "kskschedule.json"
# KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR/KSK44/skr-root-2022-q2-0.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-04-01T00:00:00 2022-04-22T00:00:00 47671,09799 20326(Klajeyz)/S
2 2022-04-11T00:00:00 2022-05-02T00:00:00 47671 20326(Klajeyz)/S
3 2022-04-21T00:00:00 2022-05-12T00:00:00 47671 20326(Klajeyz)/S
4 2022-05-01T00:00:00 2022-05-22T00:00:00 47671 20326(Klajeyz)/S
5 2022-05-11T00:00:00 2022-06-01T00:00:00 47671 20326(Klajeyz)/S
6 2022-05-21T00:00:00 2022-06-11T00:00:00 47671 20326(Klajeyz)/S
7 2022-05-31T00:00:00 2022-06-21T00:00:00 47671 20326(Klajeyz)/S
8 2022-06-10T00:00:00 2022-07-01T00:00:00 47671 20326(Klajeyz)/S
9 2022-06-20T00:00:00 2022-07-11T00:00:00 47671,20826 20326(Klajeyz)/S
```

```
SHA256 hash of SKR:
EC50BDC13BA23719F13FBEB755C3F0AB43A5672528870C78C9F395BF00958B6
>> tumor embezzle skullcap recover clockwork Pacific clamshell bottomless unwind customer
skydive underfoot indulge fascinate cowbell Apollo scenic corrosion egghead holiness Dup
ont maritime guidance retraction offload opulent classroom exodus unearth applicant endor
se potato <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0
```

```
***** Log output in ./ksrsigner-20220216-224254.log *****
root@coen:/media/HSMFD# lpadmin pp HP -o cpioes-default=5
root@coen:/media/HSMFD# printlog ksr\007si\007gner-2022021618@4254.log
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /media/KSR/
/media/KSR:
total 16
drwxr-xr-x 2 root root 16384 Feb 16 22:49 \033[0m\033[01;34mKSK44\033[0m
```

```
/media/KSR/KSK44:
total 144
-rw-r--r-- 1 root root 20369 Feb 2 23:49 skr.xml.20220216224254
-rw-r--r-- 1 root root 19598 Feb 2 23:49 ksr-root-2022-q2-0.xml
-rw-r--r-- 1 root root 1148 Feb 2 23:49 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16 22:49 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16 22:49 skr-root-2022-q2-0.xml
root@coen:/media/HSMFD# cp -pa /media/KSR/*
root@coen:/media/HSMFD# ls -ltrR
.:
total 3256
-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
```

02/17/22
00:11:30

script-20220216.log

2

```
-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 ksr-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 ksr-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
-rw-r--r-- 1 root root 8192 Aug 17 2017 \033[0m\033[01;34mKSK30-0-D_to_E\033[0m
-rw-r--r-- 1 root root 6648 Aug 17 2017 ksrsigner-20170817-214402.log
-rw-r--r-- 1 root root 8192 Aug 17 2017 \033[01;34mKSK30-1-E_to_D\033[0m
-rw-r--r-- 1 root root 6662 Aug 17 2017 ksrsigner-20170817-214602.log
-rw-r--r-- 1 root root 8192 Aug 17 2017 \033[01;34mKSK30-2-D_to_D\033[0m
-rw-r--r-- 1 root root 6355 Aug 17 2017 ksrsigner-20170817-214756.log
-rw-r--r-- 1 root root 8192 Aug 17 2017 \033[01;34mKSK30-3-C_to_C\033[0m
-rw-r--r-- 1 root root 2484 Aug 17 2017 ttyaudit-ttyUSB0-20170817-213501.log
-rw-r--r-- 1 root root 65904 Aug 17 2017 script-20170817-2.log
-rw-r--r-- 1 root root 6689 Feb 7 2018 ksrsigner-20180207-224219.log
-rw-r--r-- 1 root root 8192 Feb 7 2018 \033[01;34mKSK32-0-D_to_E\033[0m
-rw-r--r-- 1 root root 6676 Feb 7 2018 ksrsigner-20180207-224724.log
-rw-r--r-- 1 root root 8192 Feb 7 2018 \033[01;34mKSK32-1-E_to_D\033[0m
-rw-r--r-- 1 root root 6674 Feb 7 2018 ksrsigner-20180207-224920.log
-rw-r--r-- 1 root root 8192 Feb 7 2018 \033[01;34mKSK32-2-D_to_D\033[0m
-rw-r--r-- 1 root root 6367 Feb 7 2018 ksrsigner-20180207-225053.log
-rw-r--r-- 1 root root 8192 Feb 7 2018 \033[01;34mKSK32-3-C_to_C\033[0m
```

02/17/22
00:11:30

script-20220216.log

3

```
-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 0 Feb 16 22:28 script-20220216.log
-rw-r--r-- 1 root root 12851 Feb 16 22:49 ttyaudit-ttyS0-20220216-222905.log
drwxr-xr-x 2 root root 8192 Feb 16 22:49 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root 6248 Feb 16 22:49 ksrsigner-20220216-224254.log
drwxr-xr-x 2 root root 8192 Feb 16 22:49 \033[01;34mKSK44\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
```

02/17/22
00:11:30

script-20220216.log

4

```
-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

./tmp:
total 72
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Feb 16 22:49 skr.keybundle.0
-rw-r--r-- 1 root root 1768 Feb 16 22:49 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Feb 16 22:49 skr.keybundle.3

./KSK44:
total 104
-rw-r--r-- 1 root root 20369 Feb 2 23:49 skr.xml.20220216224254
-rw-r--r-- 1 root root 19598 Feb 2 23:49 ksr-root-2022-q2-0.xml
-rw-r--r-- 1 root root 1148 Feb 2 23:49 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16 22:49 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16 22:49 skr-root-2022-q2-0.xml
root@coen:/media/BSMPD# umount /m\007edia/KSR/
root@coen:/media/BSMPD# ping hsm
PING hsm (192.168.0.2) 56(84) bytes of data.
^C
--- hsm ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7171ms

root@coen:/media/BSMPD# 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=0.883 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.567 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.606 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.573 ms
^C
--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.567/0.657/0.883/0.132 ms
root@coen:/media/BSMPD# ping hsm
```


02/17/22
00:11:30

script-20220216.log

5

```
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=0.392 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.587 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.505 ms
^C
--- hsm ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2050ms
rtt min/avg/max/mdev = 0.392/0.494/0.587/0.083 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=0.417 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.575 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.573 ms
^C
--- hsm ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.417/0.521/0.575/0.078 ms
root@coen:/media/HSMFD# ksrsigner /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml
Starting: ksrsigner /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml (at Wed Feb 16 23:47:15
2022 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 2022-01-01T00:00:00 2022-01-22T00:00:00 09799,14748 20326(Klajeyz)/S
2 2022-01-11T00:00:00 2022-02-01T00:00:00 09799 20326(Klajeyz)/S
3 2022-01-21T00:00:00 2022-02-11T00:00:00 09799 20326(Klajeyz)/S
4 2022-01-31T00:00:00 2022-02-21T00:00:00 09799 20326(Klajeyz)/S
5 2022-02-10T00:00:00 2022-03-03T00:00:00 09799 20326(Klajeyz)/S
6 2022-02-20T00:00:00 2022-03-13T00:00:00 09799 20326(Klajeyz)/S
7 2022-03-02T00:00:00 2022-03-23T00:00:00 09799 20326(Klajeyz)/S
8 2022-03-12T00:00:00 2022-04-02T00:00:00 09799 20326(Klajeyz)/S
9 2022-03-22T00:00:00 2022-04-12T00:00:00 47671,09799 20326(Klajeyz)/S
...VALIDATED.

Validate and Process KSR /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml...
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-04-01T00:00:00 2022-04-22T00:00:00 47671,09799
2 2022-04-11T00:00:00 2022-05-02T00:00:00 47671
3 2022-04-21T00:00:00 2022-05-12T00:00:00 47671
4 2022-05-01T00:00:00 2022-05-22T00:00:00 47671
5 2022-05-11T00:00:00 2022-06-01T00:00:00 47671
6 2022-05-21T00:00:00 2022-06-11T00:00:00 47671
7 2022-05-31T00:00:00 2022-06-21T00:00:00 47671
8 2022-06-10T00:00:00 2022-07-01T00:00:00 47671
9 2022-06-20T00:00:00 2022-07-11T00:00:00 20826,47671
...PASSED.

SHA256 hash of KSR:
```

```
9A9FFC75B62C6FC085778080264E7171F4C1843205EEE1EBF8694D754C9FC79D
>> pupil opulent wayside impartial Scotland Chicago gremlin recipe music inception merit
intention bookshelf distortion hamlet hideaway upshot recover mural component adult unive
rse tempest underfoot Vulcan guitarist dreadful impartial drainage opulent soybean Ohio <
<
Is this correct (y/N)? y

Reading KSK schedule "normal(2017)" from "kskschedule.json"
# KSK Tag(CKA_LABEL)
1 20326(Klajeyz)/S
2 20326(Klajeyz)/S
3 20326(Klajeyz)/S
4 20326(Klajeyz)/S
5 20326(Klajeyz)/S
6 20326(Klajeyz)/S
7 20326(Klajeyz)/S
8 20326(Klajeyz)/S
9 20326(Klajeyz)/S
Generated new SKR in /media/KSR_COPY/KSK44/ksr-root-2022-q2-0.xml
# Inception Expiration ZSK Tags KSK Tag(CKA_LABEL)
1 2022-04-01T00:00:00 2022-04-22T00:00:00 47671,09799 20326(Klajeyz)/S
2 2022-04-11T00:00:00 2022-05-02T00:00:00 47671 20326(Klajeyz)/S
3 2022-04-21T00:00:00 2022-05-12T00:00:00 47671 20326(Klajeyz)/S
4 2022-05-01T00:00:00 2022-05-22T00:00:00 47671 20326(Klajeyz)/S
5 2022-05-11T00:00:00 2022-06-01T00:00:00 47671 20326(Klajeyz)/S
6 2022-05-21T00:00:00 2022-06-11T00:00:00 47671 20326(Klajeyz)/S
7 2022-05-31T00:00:00 2022-06-21T00:00:00 47671 20326(Klajeyz)/S
8 2022-06-10T00:00:00 2022-07-01T00:00:00 47671 20326(Klajeyz)/S
9 2022-06-20T00:00:00 2022-07-11T00:00:00 47671,20826 20326(Klajeyz)/S

SHA256 hash of SKR:
EC50BDC13BA23719F13FBEEB755C3F0AB43A5672528870C78C9F395BF00958B6
>> tumor embezzle skullcap recover clockwork Pacific clamshell bottomless unwind customer
skydive underfoot indulge fascinate cowbell Apollo scenic corrosion egghead holiness Dup
ont maritime guidance retraction offload opulent classroom exodus unearth applicant endor
se potato <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86_64.so.5.02 Slot=
0

***** Log output in ./ksrsigner-20220216-234715.log *****
root@coen:/media/HSMFD# lpadmin -p HP -oocopies-default=7
root@coen:/media/HSMFD# printlog $(ls -tr ks\007r\007si\007gner-202202*.log | tail -n
1)
[ 1 page * 1 copy ] sent to printer
2 lines were wrapped
root@coen:/media/HSMFD# ls -ltrR /media/KSR_COPY/
/media/KSR_COPY/:
total 16
drwxr-xr-x 2 root root 16384 Feb 16 23:49 \033[0m\033[01;34mKSK44\033[0m

/media/KSR_COPY/KSK44:
total 144
-rw-r--r-- 1 root root 20369 Feb 2 23:54 skr.xml.20220216234715
-rw-r--r-- 1 root root 19598 Feb 2 23:54 ksr-root-2022-q2-0.xml
-rw-r--r-- 1 root root 1148 Feb 2 23:54 kskschedule.json
-rw-r--r-- 1 root root 20369 Feb 16 23:49 skr.xml
-rw-r--r-- 1 root root 20369 Feb 16 23:49 ksr-root-2022-q2-0.xml
root@coen:/media/HSMFD# umount /media/K\007SR_COPY/
k888@coen:/media/HSMFD# exit
exit

Script done on Thu Feb 17 00:11:30 2022
```

```

2022-02-16T22:30:01+0000 ttyS0 Y
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0 H1903017 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0 BBL CRC32: 0xDBC9B9F2
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0 Running applicationBootLoader at 0xEFDC0000
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0 H1903017 011403 ABL 030 : Tamper Challenge Response Key
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:01+0000 ttyS0 ABL CRC32: 0xE7E0FA6A
2022-02-16T22:30:01+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 #####
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 ### ABL tamper records ###
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 #####
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 =====
2022-02-16T22:30:02+0000 ttyS0 vextoosTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 vintoosTamperCount: 6
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 vbboosTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 maxstrtempTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 minstrtempTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 meshTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 extampSMKTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 extampIMKTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 tempdiffTamperCount: 0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 pFTamperCount: 6
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 restartTamperCount: 19
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 Current tamper bitmaps:
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 =====
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 currentTamper bitmap: 0x0000 0b .... ..
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 lastTamper bitmap: 0x0080 0b .... .. 1... .. |EXT_POWER_DOWN

```

```
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 Bitmapped Change Record (most recent first):
2022-02-16T22:30:02+0000 ttyS0 =====
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0
2022-02-16T22:30:02+0000 ttyS0 Running cryptoApplication at 0xEBF00000
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0 Jumping to startup @ 0x001037B4
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0 Board is P2020RDB
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0 board_smp_init: 2 cpu
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=500000000
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:03+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0 System page at phys:0000b000 user:0000b000 kern:0000b000
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0 Starting next program at v0015183c
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0 Starting K-Series Kernel
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0 Copyright Ultra Electronics AEP. All Rights Reserved.
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0 Fri Nov 3 07:54:28 1972
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:04+0000 ttyS0 Starting auditd v2.0 ... started.
2022-02-16T22:30:04+0000 ttyS0
2022-02-16T22:30:05+0000 ttyS0 Interface 0 configured for IPv6.
2022-02-16T22:30:05+0000 ttyS0
2022-02-16T22:30:05+0000 ttyS0 Interface 0 configured for IPv4.
2022-02-16T22:30:05+0000 ttyS0
2022-02-16T22:30:05+0000 ttyS0 Interface 1 configured for IPv6.
2022-02-16T22:30:05+0000 ttyS0
2022-02-16T22:30:05+0000 ttyS0 Interface 1 configured for IPv4.
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0 add net default: gateway ::: Network is unreachable
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0 add net default: gateway 0.0.0.0: Network is unreachable
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0 Starting USB driver...
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2022-02-16T22:30:06+0000 ttyS0
2022-02-16T22:30:06+0000 ttyS0
```

```
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running DES POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 DES POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running Triple DES POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Triple DES POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running AES POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 AES POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running SHA1 POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 SHA1 POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running SHA2 POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 SHA2 POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running RandomGen POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 RandomGen POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running RSA POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 RSA POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running DSA POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 DSA POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running SEED POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 SEED POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running RIPEMD160 POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 RIPEMD160 POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running ECC POST Test
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 ECC POST Test Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Running HMAC POST Tests
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 HMAC POST Tests Passed
2022-02-16T22:30:08+0000 ttyS0
2022-02-16T22:30:08+0000 ttyS0 Audit on 3/11/1972 07:54:31 00100008
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
```

ttyaudit-ttyS0-20220216-222905.log

```
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Keyper 9860-2 Serial Number H1903017
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Memory Usage:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 RAM (free/total) 192Mb/256Mb
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Flash (free/total) 127Mb/128Mb
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 black store 524b
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 statistics 112b
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 other 116b
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 RedStore (free/total) 107Kb/128Kb
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Network Configuration:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Interface 0:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 IPv4: enabled
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 IPv6: enabled
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C4:9A / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c49a/64
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Interface 1:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 IPv4: enabled
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 IPv6: enabled
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C4:9B / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c49b/64
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 HSM Port 0: 05000
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 HSM Port 1: 03000
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Default Gateway(s): 0.0.0.0 ::
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 Software Versions:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 BBL 030 ABL 021 App 034
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 CPLD Version:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 1.9
2022-02-16T22:30:09+0000 ttyS0
```

```
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 SCR Firmware Version:
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 OROS-R2.99-R1.20
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 HmcListener: Created IPv4 socket 12 on port 3000.
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:09+0000 ttyS0 HmcListener: Created IPv6 socket 13 on port 3000.
2022-02-16T22:30:09+0000 ttyS0
2022-02-16T22:30:10+0000 ttyS0 Audit on 3/11/1972 07:54:33 00100003
2022-02-16T22:30:10+0000 ttyS0
2022-02-16T22:37:14+0000 ttyS0 Audit on 3/11/1972 08:01:37 0020006a
2022-02-16T22:37:14+0000 ttyS0
2022-02-16T22:37:33+0000 ttyS0 Audit on 3/11/1972 08:01:56 0020006a
2022-02-16T22:37:33+0000 ttyS0
2022-02-16T22:38:30+0000 ttyS0 Audit on 3/11/1972 08:02:53 00200069 0A400000B686296E
2022-02-16T22:38:30+0000 ttyS0
2022-02-16T22:38:51+0000 ttyS0 Audit on 3/11/1972 08:03:14 0020006a
2022-02-16T22:38:51+0000 ttyS0
2022-02-16T22:39:26+0000 ttyS0 Audit on 3/11/1972 08:03:49 00200069 0A4000009D86296E
2022-02-16T22:39:26+0000 ttyS0
2022-02-16T22:39:57+0000 ttyS0 Audit on 3/11/1972 08:04:21 00200069 0A4000009DC6296E
2022-02-16T22:39:57+0000 ttyS0
2022-02-16T22:40:00+0000 ttyS0
2022-02-16T22:40:00+0000 ttyS0 TcpListener: Created IPv4 socket 19 on port 5000.
2022-02-16T22:40:00+0000 ttyS0
2022-02-16T22:40:00+0000 ttyS0
2022-02-16T22:40:00+0000 ttyS0 TcpListener: Created IPv6 socket 20 on port 5000.
2022-02-16T22:40:00+0000 ttyS0
2022-02-16T22:40:00+0000 ttyS0 Audit on 3/11/1972 08:04:23 00100002
2022-02-16T22:40:00+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0 TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0 CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:43:20+0000 ttyS0
2022-02-16T22:49:40+0000 ttyS0
2022-02-16T22:49:40+0000 ttyS0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2022-02-16T22:49:40+0000 ttyS0
2022-02-16T22:54:32+0000 ttyS0 Audit on 3/11/1972 08:18:56 00200069 0A400000B686296E
```

02/17/22
00:06:31

6

ttyaudit-ttyS0-20220216-222905.log

```
2022-02-16T22:54:32+0000 ttyS0
2022-02-16T22:54:45+0000 ttyS0 Audit on 3/11/1972 08:19:08 0020006a
2022-02-16T22:54:45+0000 ttyS0
2022-02-16T22:55:18+0000 ttyS0 Audit on 3/11/1972 08:19:41 00200069 0A4000009D86296E
2022-02-16T22:55:18+0000 ttyS0
2022-02-16T22:55:43+0000 ttyS0 Audit on 3/11/1972 08:20:06 0020006a
2022-02-16T22:55:43+0000 ttyS0
2022-02-16T22:56:08+0000 ttyS0 Audit on 3/11/1972 08:20:31 00200069 0A4000009DC6296E
2022-02-16T22:56:08+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0 TcpListener: Closed IPv4 socket 19 on port 5000.
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0 TcpListener: Closed IPv6 socket 20 on port 5000.
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T22:56:10+0000 ttyS0 Audit on 3/11/1972 08:20:33 00100003
2022-02-16T22:56:10+0000 ttyS0
2022-02-16T23:00:04+0000 ttyS0
2022-02-16T23:00:04+0000 ttyS0
2022-02-16T23:00:04+0000 ttyS0 SMK v0 0080000277CF156D
2022-02-16T23:00:04+0000 ttyS0
2022-02-16T23:00:06+0000 ttyS0 Manufacturer: GemPlus
2022-02-16T23:00:06+0000 ttyS0
2022-02-16T23:00:07+0000 ttyS0 Product: MPCOS EMV
2022-02-16T23:00:07+0000 ttyS0
2022-02-16T23:00:08+0000 ttyS0 Card Size: 64 kbits
2022-02-16T23:00:08+0000 ttyS0
2022-02-16T23:00:41+0000 ttyS0
2022-02-16T23:00:41+0000 ttyS0
2022-02-16T23:00:41+0000 ttyS0 SMK v0 008000028FCF156D
2022-02-16T23:00:41+0000 ttyS0
2022-02-16T23:00:42+0000 ttyS0 Manufacturer: GemPlus
2022-02-16T23:00:42+0000 ttyS0
2022-02-16T23:00:43+0000 ttyS0 Product: MPCOS EMV
2022-02-16T23:00:43+0000 ttyS0
2022-02-16T23:00:43+0000 ttyS0 Card Size: 64 kbits
2022-02-16T23:00:43+0000 ttyS0
2022-02-16T23:05:17+0000 ttyS0 Audit on 3/11/1972 08:29:41 00200023 0A400000B8C6296E
2022-02-16T23:05:17+0000 ttyS0
2022-02-16T23:05:49+0000 ttyS0 Audit on 3/11/1972 08:30:12 00200023 0A400000B806296E
2022-02-16T23:05:49+0000 ttyS0
2022-02-16T23:06:18+0000 ttyS0 Audit on 3/11/1972 08:30:41 00200023 0A400000B846296E
2022-02-16T23:06:18+0000 ttyS0
2022-02-16T23:07:18+0000 ttyS0 Audit on 3/11/1972 08:31:42 0020002f 47800001832D2972
2022-02-16T23:07:18+0000 ttyS0
2022-02-16T23:08:05+0000 ttyS0 Audit on 3/11/1972 08:32:28 0020002f 47800001836D2972
2022-02-16T23:08:05+0000 ttyS0
2022-02-16T23:08:17+0000 ttyS0 Audit on 3/11/1972 08:32:40 00200077 47800001836D2972
2022-02-16T23:08:17+0000 ttyS0
2022-02-16T23:09:40+0000 ttyS0 Audit on 3/11/1972 08:34:03 0020002f 3880000C2CA32A76
2022-02-16T23:09:40+0000 ttyS0
2022-02-16T23:10:12+0000 ttyS0 Audit on 3/11/1972 08:34:36 0020002f 4780000183AD2972
2022-02-16T23:10:12+0000 ttyS0
2022-02-16T23:10:24+0000 ttyS0 Audit on 3/11/1972 08:34:47 00200010 4780000183AD2972
2022-02-16T23:10:24+0000 ttyS0
```

```
2022-02-16T23:11:32+0000 ttyS0 Audit on 3/11/1972 08:35:55 0020006b 47800001832D2972
2022-02-16T23:11:32+0000 ttyS0
2022-02-16T23:11:58+0000 ttyS0 Audit on 3/11/1972 08:36:21 0020006b 47800001836D2972
2022-02-16T23:11:58+0000 ttyS0
2022-02-16T23:13:06+0000 ttyS0 Audit on 3/11/1972 08:37:29 0020002d 3880000C2C632A76
2022-02-16T23:13:06+0000 ttyS0
2022-02-16T23:13:46+0000 ttyS0 Audit on 3/11/1972 08:38:09 0020002d 3880000C2C232A76
2022-02-16T23:13:46+0000 ttyS0
2022-02-16T23:14:26+0000 ttyS0 Audit on 3/11/1972 08:38:50 0020002d 39800115FEE72A76
2022-02-16T23:14:26+0000 ttyS0
2022-02-16T23:15:10+0000 ttyS0 Audit on 3/11/1972 08:39:34 0020002d 39800115FE272A76
2022-02-16T23:15:10+0000 ttyS0
2022-02-16T23:16:37+0000 ttyS0 Audit on 3/11/1972 08:41:01 00200007
2022-02-16T23:16:37+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0 H2008009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0 BBL CRC32: 0xDBC9B9F2
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0 Running applicationBootLoader at 0xEFDC0000
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0 H2008009 011403 ABL 030 : Tamper Challenge Response Key
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0 ABL CRC32: 0xE7E0FA6A
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0
2022-02-16T23:21:52+0000 ttyS0 #####
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 ### ABL tamper records ###
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 #####
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 =====
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 vextoosTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 vintoosTamperCount: 3
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 vbboosTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 maxstrtempTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 minstrtempTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 meshTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 extampSMKTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 extampIMKTamperCount: 0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 tempdiffTamperCount: 0
```


ttyaudit-ttyS0-20220216-222905.log

```
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 pfTamperCount:      3
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 restartTamperCount:  8
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 Current tamper bitmaps:
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 =====
2022-02-16T23:21:53+0000 ttyS0 currentTamper bitmap: 0x0000 0b .... ....
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 lastTamper bitmap:   0x0080 0b .... .... 1... .... |EXT_POWER_DOWN
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 Bitmapped Change Record (most recent first):
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 =====
2022-02-16T23:21:53+0000 ttyS0
2022-02-16T23:21:53+0000 ttyS0 Running cryptoApplication at 0xEBF00000
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0 Jumping to startup @ 0x001037B4
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0 Board is P2020RDB
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0 board_smp_init: 2 cpu
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=500000000
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0
2022-02-16T23:21:54+0000 ttyS0 System page at phys:0000b000 user:0000b000 kern:0000b000
2022-02-16T23:21:55+0000 ttyS0
2022-02-16T23:21:55+0000 ttyS0 Starting next program at v0015183c
2022-02-16T23:21:55+0000 ttyS0
2022-02-16T23:21:55+0000 ttyS0 Starting K-Series Kernel
2022-02-16T23:21:55+0000 ttyS0
2022-02-16T23:21:55+0000 ttyS0 Copyright Ultra Electronics AEP. All Rights Reserved.
2022-02-16T23:21:55+0000 ttyS0
2022-02-16T23:21:55+0000 ttyS0 Sat May 16 14:41:30 1970
2022-02-16T23:21:55+0000 ttyS0
2022-02-16T23:21:55+0000 ttyS0 Starting auditd v2.0 ... started.
2022-02-16T23:21:56+0000 ttyS0
2022-02-16T23:21:56+0000 ttyS0 Interface 0 configured for IPv6.
2022-02-16T23:21:56+0000 ttyS0
2022-02-16T23:21:56+0000 ttyS0 Interface 0 configured for IPv4.
2022-02-16T23:21:56+0000 ttyS0
2022-02-16T23:21:56+0000 ttyS0
2022-02-16T23:21:56+0000 ttyS0 Interface 1 configured for IPv6.
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0 Interface 1 configured for IPv4.
2022-02-16T23:21:57+0000 ttyS0
```

ttyaudit-ttyS0-20220216-222905.log

```
2022-02-16T23:21:57+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0 add net default: gateway :: Network is unreachable
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0 add net default: gateway 0.0.0.0: Network is unreachable
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0 Starting USB driver...
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:57+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running DES POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 DES POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running Triple DES POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Triple DES POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running AES POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 AES POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running SHA1 POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 SHA1 POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running SHA2 POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 SHA2 POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running RandomGen POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 RandomGen POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running RSA POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 RSA POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running DSA POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 DSA POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running SEED POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 SEED POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running RIPEMD160 POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 RIPEMD160 POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
```

```
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running ECC POST Test
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 ECC POST Test Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Running HMAC POST Tests
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 HMAC POST Tests Passed
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0 Audit on 16/5/1970 14:41:33 00100008
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:21:59+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Keyper 9860-2 Serial Number H2008009
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Memory Usage:
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 RAM (free/total) 192Mb/256Mb
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Flash (free/total) 128Mb/128Mb
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 black store 44b
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 statistics 112b
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 other 116b
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 RedStore (free/total) 107Kb/128Kb
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Network Configuration:
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Interface 0:
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 IPv4: enabled
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 IPv6: enabled
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:52 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c852/64
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Interface 1:
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 IPv4: enabled
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 IPv6: enabled
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:53 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c853/64
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 HSM Port 0: 05000
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 HSM Port 1: 03000
2022-02-16T23:22:00+0000 ttyS0
```

02/17/22
00:06:31

ttyaudit-ttyS0-20220216-222905.log

11

```
2022-02-16T23:22:00+0000 ttyS0 Default Gateway(s): 0.0.0.0 ::
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Software Versions:
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 BBL 030 ABL 021 App 034
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 CPLD Version:
2022-02-16T23:22:00+0000 ttyS0 1.9
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 SCR Firmware Version:
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 OROS-R2.99-R1.20
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:22:00+0000 ttyS0 Audit on 16/5/1970 14:41:34 00100001
2022-02-16T23:22:00+0000 ttyS0
2022-02-16T23:23:49+0000 ttyS0 Audit on 16/5/1970 14:43:22 00200035 3880000C2CA32A76
2022-02-16T23:23:49+0000 ttyS0
2022-02-16T23:24:07+0000 ttyS0 Audit on 16/5/1970 14:43:41 00200035 4780000183AD2972
2022-02-16T23:24:07+0000 ttyS0
2022-02-16T23:24:07+0000 ttyS0 Audit on 16/5/1970 14:43:41 0020000e 4780000183AD2972
2022-02-16T23:24:07+0000 ttyS0
2022-02-16T23:25:19+0000 ttyS0 Audit on 16/5/1970 14:44:53 00200023 0A400000B6C6296E
2022-02-16T23:25:19+0000 ttyS0
2022-02-16T23:25:46+0000 ttyS0 Audit on 16/5/1970 14:45:20 00200023 0A400000BA86296E
2022-02-16T23:25:46+0000 ttyS0
2022-02-16T23:26:15+0000 ttyS0 Audit on 16/5/1970 14:45:49 00200023 0A400000BAC6296E
2022-02-16T23:26:15+0000 ttyS0
2022-02-16T23:26:26+0000 ttyS0 Audit on 16/5/1970 14:46:00 00200056
2022-02-16T23:26:26+0000 ttyS0
2022-02-16T23:27:12+0000 ttyS0 Audit on 16/5/1970 14:46:46 00200081
2022-02-16T23:27:12+0000 ttyS0
2022-02-16T23:27:42+0000 ttyS0 Audit on 16/5/1970 14:47:16 00200054
2022-02-16T23:27:42+0000 ttyS0
2022-02-16T23:27:46+0000 ttyS0 Audit on 16/5/1970 14:47:20 00200028
2022-02-16T23:27:46+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 HmcListener: Created IPv4 socket 9 on port 3000.
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 HmcListener: Created IPv6 socket 11 on port 3000.
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 Audit on 16/5/1970 14:47:27 00100003
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 Audit on 16/5/1970 14:47:27 00100005
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 Shutting down daemons...
```

```
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 AuditBuffer rx'd [-1] (3)
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 shutting down audit service.
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 Terminated
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 HmcListener::accept(): No such process
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:53+0000 ttyS0 Shutting down filesystems...
2022-02-16T23:27:53+0000 ttyS0
2022-02-16T23:27:55+0000 ttyS0
2022-02-16T23:27:55+0000 ttyS0
2022-02-16T23:27:55+0000 ttyS0 H2008009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2022-02-16T23:27:55+0000 ttyS0
2022-02-16T23:27:55+0000 ttyS0 BBL CRC32: 0xDBC9B9F2
2022-02-16T23:27:55+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 Running applicationBootLoader at 0xEFDC0000
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 H2008009 011403 ABL 030 : Tamper Challenge Response Key
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 ABL CRC32: 0xE7E0FA6A
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 #####
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 ### ABL tamper records ###
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 #####
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 =====
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 vextoosTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 vintoosTamperCount: 3
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 vbboosTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 maxstrtempTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 minstrtempTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 meshTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 extampSMKTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 extampIMKTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 tempdiffTamperCount: 0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 pfTamperCount: 3
2022-02-16T23:27:56+0000 ttyS0
```

```
2022-02-16T23:27:56+0000 ttyS0 restartTamperCount:      8
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 Current tamper bitmaps:
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 =====
2022-02-16T23:27:56+0000 ttyS0 currentTamper bitmap:  0x0000 0b .... .... ....
2022-02-16T23:27:56+0000 ttyS0 lastTamper bitmap:    0x0080 0b .... .... 1... .... |EXT_POWER_DOWN
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 Bitmapped Change Record (most recent first):
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0 =====
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:56+0000 ttyS0
2022-02-16T23:27:57+0000 ttyS0 Running cryptoApplication at 0xEBF00000
2022-02-16T23:27:57+0000 ttyS0
2022-02-16T23:27:57+0000 ttyS0 Jumping to startup @ 0x001037B4
2022-02-16T23:27:57+0000 ttyS0
2022-02-16T23:27:57+0000 ttyS0 Board is P2020RDB
2022-02-16T23:27:57+0000 ttyS0 board_smp_init: 2 cpu
2022-02-16T23:27:57+0000 ttyS0
2022-02-16T23:27:57+0000 ttyS0
2022-02-16T23:27:57+0000 ttyS0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=500000000
2022-02-16T23:27:57+0000 ttyS0
2022-02-16T23:27:58+0000 ttyS0
2022-02-16T23:27:58+0000 ttyS0 System page at phys:0000b000 user:0000b000 kern:0000b000
2022-02-16T23:27:58+0000 ttyS0
2022-02-16T23:27:58+0000 ttyS0 Starting next program at v0015183c
2022-02-16T23:27:58+0000 ttyS0
2022-02-16T23:27:58+0000 ttyS0 Starting K-Series Kernel
2022-02-16T23:27:58+0000 ttyS0
2022-02-16T23:27:58+0000 ttyS0 Copyright Ultra Electronics AEP. All Rights Reserved.
2022-02-16T23:27:58+0000 ttyS0
2022-02-16T23:27:59+0000 ttyS0 Sat May 16 14:47:33 1970
2022-02-16T23:27:59+0000 ttyS0
2022-02-16T23:27:59+0000 ttyS0 Starting auditd v2.0 ... started.
2022-02-16T23:27:59+0000 ttyS0
2022-02-16T23:27:59+0000 ttyS0 Interface 0 configured for IPv6.
2022-02-16T23:27:59+0000 ttyS0
2022-02-16T23:27:59+0000 ttyS0 Interface 0 configured for IPv4.
2022-02-16T23:27:59+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 Interface 1 configured for IPv6.
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 Interface 1 configured for IPv4.
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 add net default: gateway :: Network is unreachable
```

```
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 add net default: gateway 0.0.0.0: Network is unreachable
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 Starting USB driver...
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:00+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running DES POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 DES POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running Triple DES POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Triple DES POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running AES POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 AES POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running SHA1 POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 SHA1 POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running SHA2 POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 SHA2 POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running RandomGen POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 RandomGen POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running RSA POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 RSA POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running DSA POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 DSA POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running SEED POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 SEED POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running RIPEMD160 POST Test
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 RIPEMD160 POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running ECC POST Test
2022-02-16T23:28:02+0000 ttyS0
```

```
2022-02-16T23:28:02+0000 ttyS0 ECC POST Test Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 Running HMAC POST Tests
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0 HMAC POST Tests Passed
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:02+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Keyper 9860-2 Serial Number H2008009
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Memory Usage:
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 RAM (free/total) 192Mb/256Mb
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Flash (free/total) 128Mb/128Mb
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 black store 272b
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 statistics 112b
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 other 116b
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 RedStore (free/total) 107Kb/128Kb
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Network Configuration:
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Interface 0:
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 IPv4: enabled
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 IPv6: enabled
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:52 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c852/64
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Interface 1:
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 IPv4: enabled
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 IPv6: enabled
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:53 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c853/64
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 HSM Port 0: 05000
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 HSM Port 1: 03000
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Default Gateway(s): 0.0.0.0 ::
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Software Versions:
```



```
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 BBL 030 ABL 021 App 034
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 CPLD Version:
2022-02-16T23:28:03+0000 ttyS0 1.9
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 SCR Firmware Version:
2022-02-16T23:28:03+0000 ttyS0 OROS-R2.99-R1.20
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 HmcListener: Created IPv4 socket 9 on port 3000.
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 HmcListener: Created IPv6 socket 10 on port 3000.
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Audit on 16/5/1970 14:47:37 00100003
2022-02-16T23:28:03+0000 ttyS0
2022-02-16T23:28:03+0000 ttyS0 Audit on 16/5/1970 14:48:25 0020006b 47800001832D2972
2022-02-16T23:28:51+0000 ttyS0
2022-02-16T23:28:51+0000 ttyS0 Audit on 16/5/1970 14:48:53 0020006b 47800001836D2972
2022-02-16T23:29:19+0000 ttyS0
2022-02-16T23:29:19+0000 ttyS0
2022-02-16T23:29:19+0000 ttyS0 Audit on 16/5/1970 14:49:15 00200039
2022-02-16T23:29:41+0000 ttyS0
2022-02-16T23:29:41+0000 ttyS0
2022-02-16T23:29:56+0000 ttyS0 Audit on 16/5/1970 14:49:29 0020003b
2022-02-16T23:29:56+0000 ttyS0
2022-02-16T23:29:56+0000 ttyS0 Audit on 16/5/1970 14:49:48 00200041
2022-02-16T23:30:14+0000 ttyS0
2022-02-16T23:30:14+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 HSM Status
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Keyper 9860-2
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Serial Number H2008009
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Date(dd/mm/yyyy) 16/5/1970 Time 14:50:33
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Software Versions:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 BBL 030 ABL 021 App 034
2022-02-16T23:30:59+0000 ttyS0
```

```
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 CPLD Version:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 1.9
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 SCR Firmware Version:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 OROS-R2.99-R1.20
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Memory Usage:
2022-02-16T23:30:59+0000 ttyS0 RAM (free/total) 192Mb/256Mb
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Flash (free/total) 128Mb/128Mb
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 black store 452b
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 statistics 112b
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 other 116b
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 RedStore (free/total) 107Kb/128Kb
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Network Configuration:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Interface 0:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 IPv4: enabled
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 IPv6: enabled
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:52 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c852/64
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 capabilities tx=0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 enabled=0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 address: 00:e0:6c:00:c8:52
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 media: Ethernet none
```

```
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      inet 192.168.0.2 netmask 0xffffffff broadcast 192.168.0.255
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      inet6 2001::2e0:6cff:fe00:c852 prefixlen 64
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      inet6 fe80::2e0:6cff:fe00:c852%tsec0 prefixlen 64 scopeid 0x2
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      Interface 1:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      IPv4: enabled
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      IPv6: enabled
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      MAC/IP address(es): 00:E0:6C:00:C8:53 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c853/64
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      tsec1: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      capabilities tx=0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      enabled=0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      address: 00:e0:6c:00:c8:53
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      media: Ethernet none
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      inet 192.168.1.2 netmask 0xffffffff broadcast 192.168.1.255
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      inet6 2001::1:2e0:6cff:fe00:c853 prefixlen 64
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      inet6 fe80::2e0:6cff:fe00:c853%tsec1 prefixlen 64 scopeid 0x3
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      HSM Port 0: 05000
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      HSM Port 1: 03000
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      Default Gateway(s): 0.0.0.0 ::
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      Current HSM State: Secured Off-line
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      Modes: (1=Enabled 0=Disabled)
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      Global Key Export    1 App Key Import      0 App Key Export      0 Asymmetric Key Gen  1
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      Symmetric Key Gen    1 Symmetric Key Derive 0 Signing              1 Signature Verify    1
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0      MAC Generation       1 MAC Verification    1 Encrypt / Decrypt    1 Delete Asym Key     1
2022-02-16T23:30:59+0000 ttyS0
```

ttyaudit-ttyS0-20220216-222905.log

```
2022-02-16T23:30:59+0000 ttyS0 Delete Sym Key      1 Output Key Details  1 Output Key Summary  1 Suite B Algorithms  1
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Non Suite B Algs    1 Auto Online        0 Remote Management  0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Other Modes:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 AES SMK             Set Offline          FIPS Mode
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Battery ok
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 #####
2022-02-16T23:30:59+0000 ttyS0 ###      ABL tamper records      ###
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 #####
2022-02-16T23:30:59+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 =====
2022-02-16T23:30:59+0000 ttyS0 vextoosTamperCount:    0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 vintoosTamperCount:    0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 vbboosTamperCount:    0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 maxstrtempTamperCount: 0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 minstrtempTamperCount: 0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 meshTamperCount:      0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 extampSMKTamperCount: 0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 extampIMKTamperCount: 0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 tempdiffTamperCount:  0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 pfTamperCount:        0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 restartTamperCount:   0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Current tamper bitmaps:
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 =====
2022-02-16T23:30:59+0000 ttyS0 currentTamper bitmap: 0x0000 0b .....
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 lastTamper bitmap:    0x0000 0b .....
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
```

```
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 Bitmapped Change Record (most recent first):
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 \000=====
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 DRBG Instantiate Health Test On Demand Passed
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 DRBG Generate Health Test On Demand Passed
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:30:59+0000 ttyS0 DRBG Reseed Health Test On Demand Passed
2022-02-16T23:30:59+0000 ttyS0
2022-02-16T23:36:28+0000 ttyS0 Audit on 16/5/1970 14:56:01 0020006b 47800001832D2972
2022-02-16T23:36:28+0000 ttyS0
2022-02-16T23:36:28+0000 ttyS0 Audit on 16/5/1970 14:56:22 0020006b 47800001836D2972
2022-02-16T23:36:48+0000 ttyS0
2022-02-16T23:36:48+0000 ttyS0 Audit on 16/5/1970 14:56:59 00200025 3880000C2C632A76
2022-02-16T23:37:25+0000 ttyS0
2022-02-16T23:37:25+0000 ttyS0 Audit on 16/5/1970 14:57:14 00200025 3880000C2C232A76
2022-02-16T23:37:40+0000 ttyS0
2022-02-16T23:37:40+0000 ttyS0 Audit on 16/5/1970 14:57:17 00200005
2022-02-16T23:37:43+0000 ttyS0
2022-02-16T23:37:43+0000 ttyS0 Audit on 16/5/1970 14:58:47 00200016 Klajeyz
2022-02-16T23:39:13+0000 ttyS0
2022-02-16T23:39:13+0000 ttyS0 Audit on 16/5/1970 14:58:47 00200015 47800001BDED2972
2022-02-16T23:39:13+0000 ttyS0
2022-02-16T23:39:13+0000 ttyS0 Audit on 16/5/1970 14:58:47 00200018
2022-02-16T23:39:13+0000 ttyS0
2022-02-16T23:43:07+0000 ttyS0 Audit on 16/5/1970 15:02:41 00200069 0A400000B686296E
2022-02-16T23:43:07+0000 ttyS0
2022-02-16T23:43:31+0000 ttyS0 Audit on 16/5/1970 15:03:05 0020006a
2022-02-16T23:43:31+0000 ttyS0
2022-02-16T23:44:01+0000 ttyS0 Audit on 16/5/1970 15:03:35 00200069 0A4000009D86296E
2022-02-16T23:44:01+0000 ttyS0
2022-02-16T23:44:27+0000 ttyS0 Audit on 16/5/1970 15:04:01 00200069 0A4000009DC6296E
2022-02-16T23:44:28+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0 TcpListener: Created IPv4 socket 20 on port 5000.
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0 TcpListener: Created IPv6 socket 21 on port 5000.
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:44:30+0000 ttyS0 Audit on 16/5/1970 15:04:04 00100002
2022-02-16T23:44:30+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0 TcpListener: Accepted connection on socket 22 from address 192.168.0.1.
2022-02-16T23:47:32+0000 ttyS0
```

```

2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0 CryptoTask: Closing connection on socket 22 from address 192.168.0.1.
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:47:32+0000 ttyS0 TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2022-02-16T23:47:32+0000 ttyS0
2022-02-16T23:49:04+0000 ttyS0
2022-02-16T23:49:04+0000 ttyS0
2022-02-16T23:49:04+0000 ttyS0 CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2022-02-16T23:49:04+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0 H2008009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0 BBL CRC32: 0xDB9B9F2
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0 Running applicationBootLoader at 0xEFDC0000
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0 H2008009 011403 ABL 030 : Tamper Challenge Response Key
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:33+0000 ttyS0 ABL CRC32: 0xE7E0FA6A
2022-02-16T23:53:33+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 #####
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 ### ABL tamper records ###
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 #####
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 Current Tamper Counts (decimal 0-255):
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 =====
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 vextoosTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 vintoosTamperCount: 3
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 vbboosTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 maxstrtempTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 minstrtempTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 meshTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 extampSMKTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 extampIMKTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 tempdiffTamperCount: 0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 pfTamperCount: 3

```

```
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 restartTamperCount: 10
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 Current tamper bitmaps:
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 =====
2022-02-16T23:53:34+0000 ttyS0 currentTamper bitmap: 0x0000 0b .... .... ....
2022-02-16T23:53:34+0000 ttyS0 lastTamper bitmap: 0x0080 0b .... .... 1... .... |EXT_POWER_DOWN
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 Bitmapped Change Record (most recent first):
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 =====
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0
2022-02-16T23:53:34+0000 ttyS0 Running cryptoApplication at 0xEBF00000
2022-02-16T23:53:35+0000 ttyS0
2022-02-16T23:53:35+0000 ttyS0 Jumping to startup @ 0x001037B4
2022-02-16T23:53:35+0000 ttyS0
2022-02-16T23:53:35+0000 ttyS0 Board is P2020RDB
2022-02-16T23:53:35+0000 ttyS0 board_smp_init: 2 cpu
2022-02-16T23:53:35+0000 ttyS0
2022-02-16T23:53:35+0000 ttyS0 Cpu_clk=1000000000, Sys_clk=1000000000, CCB=500000000
2022-02-16T23:53:35+0000 ttyS0
2022-02-16T23:53:35+0000 ttyS0
2022-02-16T23:53:35+0000 ttyS0 System page at phys:0000b000 user:0000b000 kern:0000b000
2022-02-16T23:53:36+0000 ttyS0
2022-02-16T23:53:36+0000 ttyS0 Starting next program at v0015183c
2022-02-16T23:53:36+0000 ttyS0
2022-02-16T23:53:36+0000 ttyS0 Starting K-Series Kernel
2022-02-16T23:53:36+0000 ttyS0
2022-02-16T23:53:36+0000 ttyS0 Copyright Ultra Electronics AEP. All Rights Reserved.
2022-02-16T23:53:36+0000 ttyS0
2022-02-16T23:53:36+0000 ttyS0 Sat May 16 15:13:11 1970
2022-02-16T23:53:36+0000 ttyS0
2022-02-16T23:53:36+0000 ttyS0 Starting auditd v2.0 ... started.
2022-02-16T23:53:37+0000 ttyS0
2022-02-16T23:53:37+0000 ttyS0 Interface 0 configured for IPv6.
2022-02-16T23:53:37+0000 ttyS0
2022-02-16T23:53:37+0000 ttyS0 Interface 0 configured for IPv4.
2022-02-16T23:53:37+0000 ttyS0
2022-02-16T23:53:37+0000 ttyS0 Interface 1 configured for IPv6.
2022-02-16T23:53:37+0000 ttyS0
2022-02-16T23:53:37+0000 ttyS0 Interface 1 configured for IPv4.
2022-02-16T23:53:38+0000 ttyS0
2022-02-16T23:53:38+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T23:53:38+0000 ttyS0
```

```
2022-02-16T23:53:38+0000 ttyS0 add net default: gateway ::: Network is unreachable
2022-02-16T23:53:38+0000 ttyS0
2022-02-16T23:53:38+0000 ttyS0 route: writing to routing socket: Network is unreachable
2022-02-16T23:53:38+0000 ttyS0
2022-02-16T23:53:38+0000 ttyS0 add net default: gateway 0.0.0.0: Network is unreachable
2022-02-16T23:53:38+0000 ttyS0
2022-02-16T23:53:38+0000 ttyS0 Starting USB driver...
2022-02-16T23:53:38+0000 ttyS0
2022-02-16T23:53:38+0000 ttyS0 9860 v3.4 Keyper Application - May 19 2017 15:48:58
2022-02-16T23:53:38+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running DES POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 DES POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running Triple DES POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Triple DES POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running AES POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 AES POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running SHA1 POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 SHA1 POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running SHA2 POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 SHA2 POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running RandomGen POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 RandomGen POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running RSA POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 RSA POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running DSA POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 DSA POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running SEED POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 SEED POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running RIPEMD160 POST Test
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 RIPEMD160 POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running ECC POST Test
```



```
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 ECC POST Test Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Running HMAC POST Tests
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 HMAC POST Tests Passed
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0 Audit on 16/5/1970 15:13:14 00100008
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:40+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Keyper 9860-2 Serial Number H2008009
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Memory Usage:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 RAM (free/total) 192Mb/256Mb
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Flash (free/total) 128Mb/128Mb
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 black store 524b
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 statistics 112b
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 other 116b
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 RedStore (free/total) 107Kb/128Kb
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Network Configuration:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Interface 0:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 IPv4: enabled
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 IPv6: enabled
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:52 / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c852/64
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Interface 1:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 IPv4: enabled
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 IPv6: enabled
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 MAC/IP address(es): 00:E0:6C:00:C8:53 / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c853/64
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 HSM Port 0: 05000
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 HSM Port 1: 03000
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Default Gateway(s): 0.0.0.0 ::
2022-02-16T23:53:41+0000 ttyS0
```




```
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Software Versions:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 BBL 030 ABL 021 App 034
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 CPLD Version:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 1.9
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 SCR Firmware Version:
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 OROS-R2.99-R1.20
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 HmcListener: Created IPv4 socket 12 on port 3000.
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 HmcListener: Created IPv6 socket 13 on port 3000.
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:53:41+0000 ttyS0 Audit on 16/5/1970 15:13:15 00100003
2022-02-16T23:53:41+0000 ttyS0
2022-02-16T23:54:52+0000 ttyS0 Audit on 16/5/1970 15:14:26 0020006b 47800001832D2972
2022-02-16T23:54:52+0000 ttyS0
2022-02-16T23:55:17+0000 ttyS0 Audit on 16/5/1970 15:14:51 0020006b 47800001836D2972
2022-02-16T23:55:17+0000 ttyS0
2022-02-16T23:56:46+0000 ttyS0 Audit on 16/5/1970 15:16:20 0020002d 3880000C2C632A76
2022-02-16T23:56:46+0000 ttyS0
2022-02-16T23:57:30+0000 ttyS0 Audit on 16/5/1970 15:17:04 0020002d 3880000C2C232A76
2022-02-16T23:57:30+0000 ttyS0
2022-02-16T23:58:09+0000 ttyS0 Audit on 16/5/1970 15:17:43 0020002d 39800115FEE72A76
2022-02-16T23:58:09+0000 ttyS0
2022-02-16T23:58:47+0000 ttyS0 Audit on 16/5/1970 15:18:21 0020002d 39800115FE272A76
2022-02-16T23:58:47+0000 ttyS0
2022-02-17T00:02:06+0000 ttyS0 Audit on 16/5/1970 15:21:40 00200023 0A400000B8C6296E
2022-02-17T00:02:06+0000 ttyS0
2022-02-17T00:02:30+0000 ttyS0 Audit on 16/5/1970 15:22:05 00200023 0A400000B806296E
2022-02-17T00:02:30+0000 ttyS0
2022-02-17T00:02:59+0000 ttyS0 Audit on 16/5/1970 15:22:33 00200023 0A400000B846296E
2022-02-17T00:02:59+0000 ttyS0
2022-02-17T00:04:04+0000 ttyS0 Audit on 16/5/1970 15:23:38 00200070 47800001832D2972
2022-02-17T00:04:04+0000 ttyS0
2022-02-17T00:04:52+0000 ttyS0 Audit on 16/5/1970 15:24:26 00200070 47800001836D2972
2022-02-17T00:04:52+0000 ttyS0
2022-02-17T00:05:57+0000 ttyS0 Audit on 16/5/1970 15:25:31 0020002c 3880000C2CA32A76
2022-02-17T00:05:57+0000 ttyS0
2022-02-17T00:06:31+0000 ttyS0 Audit on 16/5/1970 15:26:05 0020002c 4780000183AD2972
2022-02-17T00:06:31+0000 ttyS0
```

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.	JD	00:29
22	<p>CA performs the following steps:</p> <ul style="list-style-type: none"> a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and laptop serial number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the laptop TEB on the cart. <p>Laptop3: TEB # BB81420073 / Service Tag # C8SVSG2</p>	JD	00:30

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
23	<p>CA perform the following steps sequentially for the COs listed below:</p> <ul style="list-style-type: none"> a) Gather the OP TEB and plastic case prepared for the CO. b) Take the CO's OP card from the card holder and place it inside of the plastic case. c) Place the plastic case into the prepared TEB, read aloud the TEB number and description, then seal it. d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory. e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. f) Repeat steps a) to e) for the 2 SO cards respectively, ensuring they're facing outward in the plastic case and placed into the prepared SO TEB. g) IW writes the date and time, then signs the table of IW's script, then CA initials the entry. h) IW places the TEBs on the ceremony table. i) Repeat steps for the remaining COs' credentials on the list. <p>CO4: Carlos Martinez OP TEB # BB91951257 SO TEB # BB91951254</p> <p>CO5: Olafur Gudmundsson OP TEB # BB91951256 SO TEB # BB91951253</p> <p>CO6: Nicolas Antonello OP TEB # BB91951255 SO TEB # BB91951252</p>	JD	00:39

CO	Card Type	TEB #	Printed Name	Signature	Date	Time	CA Initials
CO4	OP 4 of 7 SO 4 of 7	OP TEB # BB91951257 SO TEB # BB91951254	Jonathan Denison		2022 Feb 16 ¹⁷	00:38	GL
CO5	OP 5 of 7 SO 5 of 7	OP TEB # BB91951256 SO TEB # BB91951253	Jonathan Denison		2022 Feb 16 ¹⁷	00:38	GL
CO6	OP 6 of 7 SO 6 of 7	OP TEB # BB91951255 SO TEB # BB91951252	Jonathan Denison		2022 Feb 16 ¹⁷	00:38	GL

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	00:41
25	SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.	JD	00:42
26	SSC1 removes the safe log, then writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	JD	00:43
27	CA performs the following steps to return each piece of equipment to the safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where "Return" is indicated. d) IW verifies the safe log entry, then initials it. HSM5W: TEB # BB51184290 HSM6W: TEB # BB51184288 Laptop3: TEB # BB81420073 OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951259 KSK-2017: TEB # BB91951258	JD	00:46

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	00:47
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	00:47
30	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	JD	00:48

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
31	CA transport the guard key, a flashlight, and with IW escort SSC2 into Tier 5 (Safe Room.)	JD	00:49
32	SSC2 opens Safe #2 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.	JD	00:50
33	SSC2 removes the safe log, then writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	JD	00:51

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

Step	Activity	Initials	Time
34	<p>IW performs the following steps sequentially to return the required TEBs:</p> <ul style="list-style-type: none"> a) IW reads aloud the TEB number, then verifies the integrity of the TEB while showing it to the audit camera above b) After the CA operates the guard key in the bottom lock, IW uses the CO's tenant key to operate the top lock and opens the CO's safe deposit box. c) IW reads aloud the safe deposit box number, places the TEB inside, then closes and locks the safe deposit box with assistance from the CA. d) IW writes the date and time, then signs the safe log where "Return" is indicated. e) CA verifies the completed safe log entry, then initials it. <p>CO4: Carlos Martinez Box # 1068 1791 OP TEB # BB91951257 SO TEB # BB91951254</p> <p>CO5: Olafur Gudmundsson Box # 1789 OP TEB # BB91951256 SO TEB # BB91951253</p> <p>CO6: Nicolas Antoniello Box # 1073 OP TEB # BB91951255 SO TEB # BB91951252</p>	JD	00:59

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	01:00
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	01:00
37	CA, IW, and SSC2 leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	JD	01:01

Place Crypto Officer Keys into TEBs

Step	Activity	Initials	Time
38	<p>CA performs the following steps sequentially for the COs key listed below:</p> <ul style="list-style-type: none"> a) Gather the CO key TEB and envelope prepared for the CO. b) IW gives the CO key to CA who then places it inside of the envelope. c) Place the envelope into the prepared TEB, read aloud the TEB number and description, then seal it. d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory. e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. f) Repeat steps for remaining COs' keys on the list. <p>CO4: Carlos Martinez Key TEB # BB91951251 AND 8846584697 (SEE EXCEPTION)</p> <p>CO5: Olafur Gudmundsson Key TEB # BB91951250</p> <p>CO6: Nicolas Antonello Key TEB # BB91951249</p> <p>Note: The COs' keys will be promptly returned to the COs who will sign a second key declaration form confirming receipt. The completed declaration forms will be available on the IANA web page along with the standard post-ceremony materials.</p>	JO	01:17

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Carlos Martinez** hereby attest that my safe deposit box key for safe deposit box **#1068** located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951317** before transmitting the key via courier.

I witnessed the key's extraction from the courier envelope when it was required to perform disaster recovery operations in an audited ceremony environment. The shipping envelope indicated that it had been inspected by U.S. border patrol and customs prior to delivery. The TEB was examined by the Ceremony Administrator and found to be tampered before the key was used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization when the key ceremony script required use of the safe deposit box key. Due to the apparent tampering of my key in transit, it was decided to transfer my credentials to the vacant safe deposit box **#1791** utilizing a new and unused tenant key set. After my credentials were returned to the safe deposit box, I remotely witnessed the first of my new keys placed into **TEB #BB91951251** before the key was returned to me. Upon receipt of this first new key, the CBO team have agreed to transmit the second of two tenant keys to me in **TEB #46584697**.

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

Printed Name Carlos MARTINEZ

Signature Carlos Martinez

Date 2/22/2022

Crypto Officer Safe Deposit Box Key Declaration

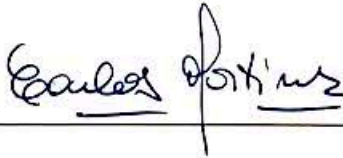
Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Carlos Martinez** hereby attest that my safe deposit box key for safe deposit box #1068 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951317** before transmitting the key via courier.

I witnessed the key's extraction from the courier envelope when it was required to perform disaster recovery operations in an audited ceremony environment. The shipping envelope indicated that it had been inspected by U.S. border patrol and customs prior to delivery. The TEB was examined by the Ceremony Administrator and found to be tampered before the key was used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization when the key ceremony script required use of the safe deposit box key. Due to the apparent tampering of my key in transit, it was decided to transfer my credentials to the vacant safe deposit box #1791 utilizing a new and unused tenant key set. After my credentials were returned to the safe deposit box, I remotely witnessed the first of my new keys placed into **TEB #BB91951251** before the key was returned to me. I have received this first new tenant key, confirmed receipt of the first key, and the CBO team subsequently transmitted the second of two tenant keys to me in **TEB #46584697**.

I attest the second new safe deposit box key arrived with indications of tampering, and after providing evidence to the CBO team, we decided together to schedule a safe deposit box rotation for my credentials at the next opportunity during a KSK ceremony.

Printed Name CARLOS MARCELO MARTINEZ

Signature 

Date March 11, 2022

Crypto Officer Safe Deposit Box Key Declaration


Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Olafur Gudmundsson** hereby attest that my safe deposit box key for safe deposit box #1789 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951315** before transmitting the key via courier.

I witnessed the key's extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into **TEB #BB91951250** before the key was returned to me.

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

Printed Name OLAFUR GUAMUNDSSON

Signature 

Date 2022/2/18

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Nicolas Antoniello** hereby attest that my safe deposit box key for safe deposit box #1073 located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in TEB #BB91951313 before transmitting the key via courier.

I witnessed the key's extraction from the courier envelope while still safeguarded within its enclosed TEB until the time it was required to perform disaster recovery operations in an audited ceremony environment. The TEB was examined by the Ceremony Administrator before the key was removed from its TEB and used to operate the safe deposit box lock. I remotely monitored the use of my key, and provided authorization when the key ceremony script required use of the safe deposit box key. After my credentials were returned to the safe deposit box, I remotely witnessed my key placed into TEB #BB91951249 before the key was returned to me.

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

Printed Name Nicolas Antoniello

Signature 

Date 22/FEB/2022

Crypto Officer Safe Deposit Box Key Declaration

Due to the invocation of a disaster recovery response by the Root Zone KSK Operator, in order to allow the proper conduct of a Root KSK ceremony with less than the standard minimum of three Crypto Officers in-person, I **Joao Luis Silva Damas** hereby attest that my safe deposit box key for safe deposit box **#1069** located within Safe #2 at the key management facility in El Segundo, CA was voluntarily transmitted to the Root Zone KSK Operator and subsequently returned to me.

I attest to packaging the safe deposit box key in **TEB #BB91951319** before transmitting the key via courier.

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

Printed Name JOAO LUIS SILVA DAMAS

Signature Joao Luis Silva Damas

Date 21-FEB-2022

Act 8: Close the Key Signing Ceremony

The CA will finish the ceremony by performing the following steps:

- Read any exceptions that occurred during the ceremony
- Call the ceremony participants to sign the IW's script
- Stop the online streaming and video recording
- Ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Prepare the audit bundle materials

Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.	JD	01:20
2	CA asks any COs who are participating remotely if they have any concerns pertaining to the ceremony or exceptions which may have occurred.	JD	01:21
3	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. All signatories declare that this script is a true and accurate record of the ceremony.	JD	01:22
4	CA reviews IW's script, then signs the participants list.	JD	01:27
5	IW signs the list and records the completion time.	JD	01:27

Stop Online Streaming and Post Ceremony Information

Step	Activity	Initials	Time
6	CA acknowledges the participation of the online participants, then notifies the SA to stop the online streaming.	JD	01:28
7	CA informs onsite participants of post ceremony activities.	JD	01:28
8	Ceremony participants take a group photo.	JD	01:33
9	CA acknowledges the participation of the COs, RZM, and Auditors in the call, then stops the call.	JD	01:33

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

Step	Activity	Initials	Time
10	RKOS ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.) SA, IW, and CA must remain in Tier 4 (Key Ceremony Room.)	JD	01:45
11	CA requests that an SA stop the audit camera video recording.	JD	01:45

Bundle Audit Materials

Step	Activity	Initials	Time
12	<p>IW makes a copy of their script for off-site audit bundle containing:</p> <ul style="list-style-type: none"> a) Output of signer system – HSMFD. b) Copy of IW's key ceremony script. c) Audio-visual recording from the audit cameras. d) Logs from the Physical Access Control System and Intrusion Detection System: Range: 20210211 00:00:00 to 20220217 00:00:00 UTC e) IW's attestation (See Appendix C on page 44). f) SA's attestation (See Appendix D on page 45 and Appendix E on page 46). <p>All TEBs are labeled Root DNSSEC KSK Ceremony 44, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>	JD	02:50

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/sk-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/sk-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/sk-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/sk-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 sk-tools-0.1.0coen_amd64.deb`
Then extract the files with `tar -zxvf data.tar.xz`
The file will be located in the directory: `./opt/icann/bin/`

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes during the ceremony and attestation. See Appendix C on page 44.

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 45.

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 46. 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: 2022 Feb 17

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:

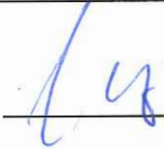
- a) There were NO discrepancies found in the system configurations, assigned authorizations and audit logs.
- b) Aside from the date filter that is applicable to some reports, there were NO other filters applied.

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: **20210211 00:00:00 to 20220217 00:00:00 UTC.**

SA: Josh Jenkins

Signature: 

Date: 2022 Feb/17

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.

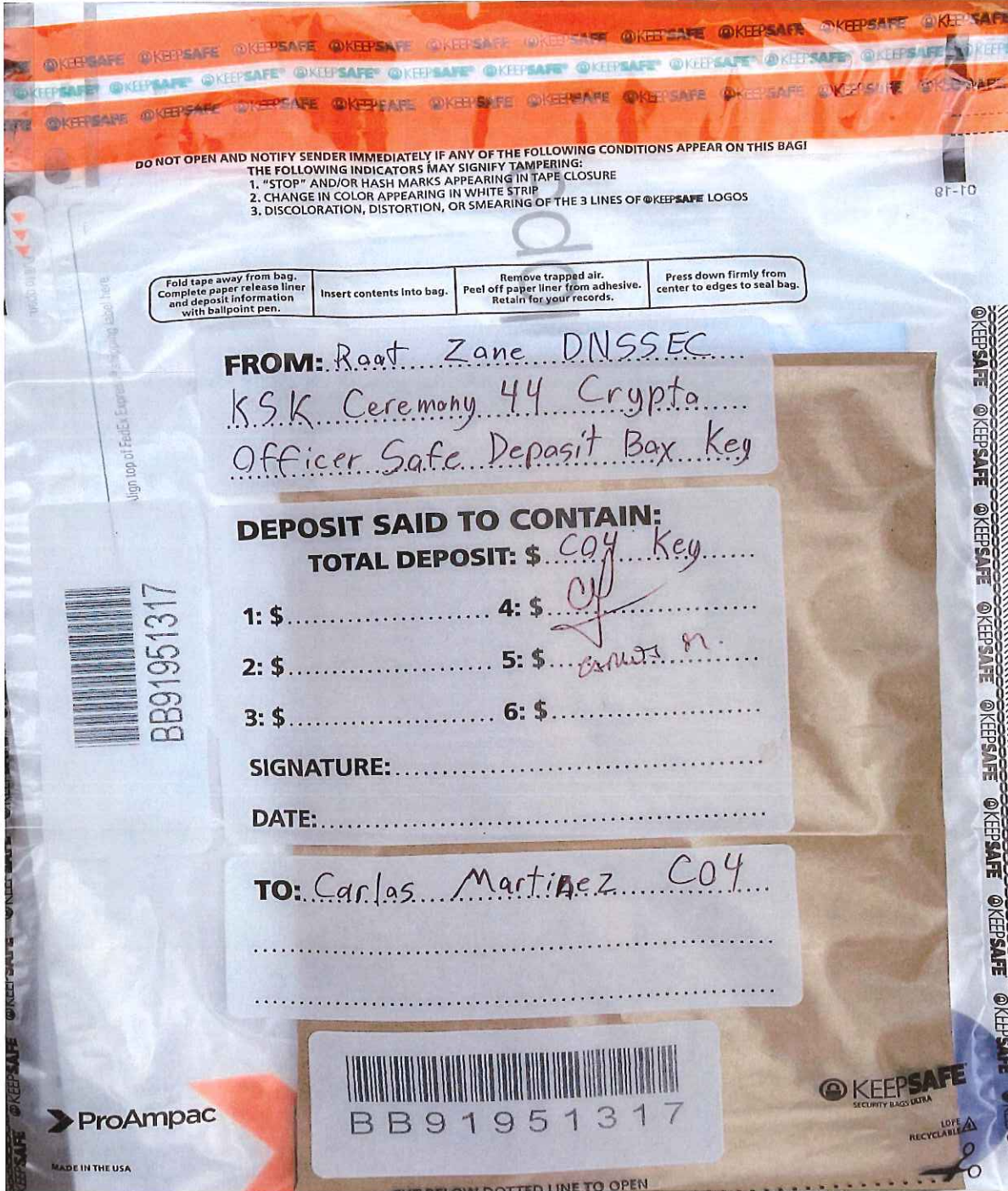
SA: Josh Jenkins

Signature: 

Date: 2022 Feb 17

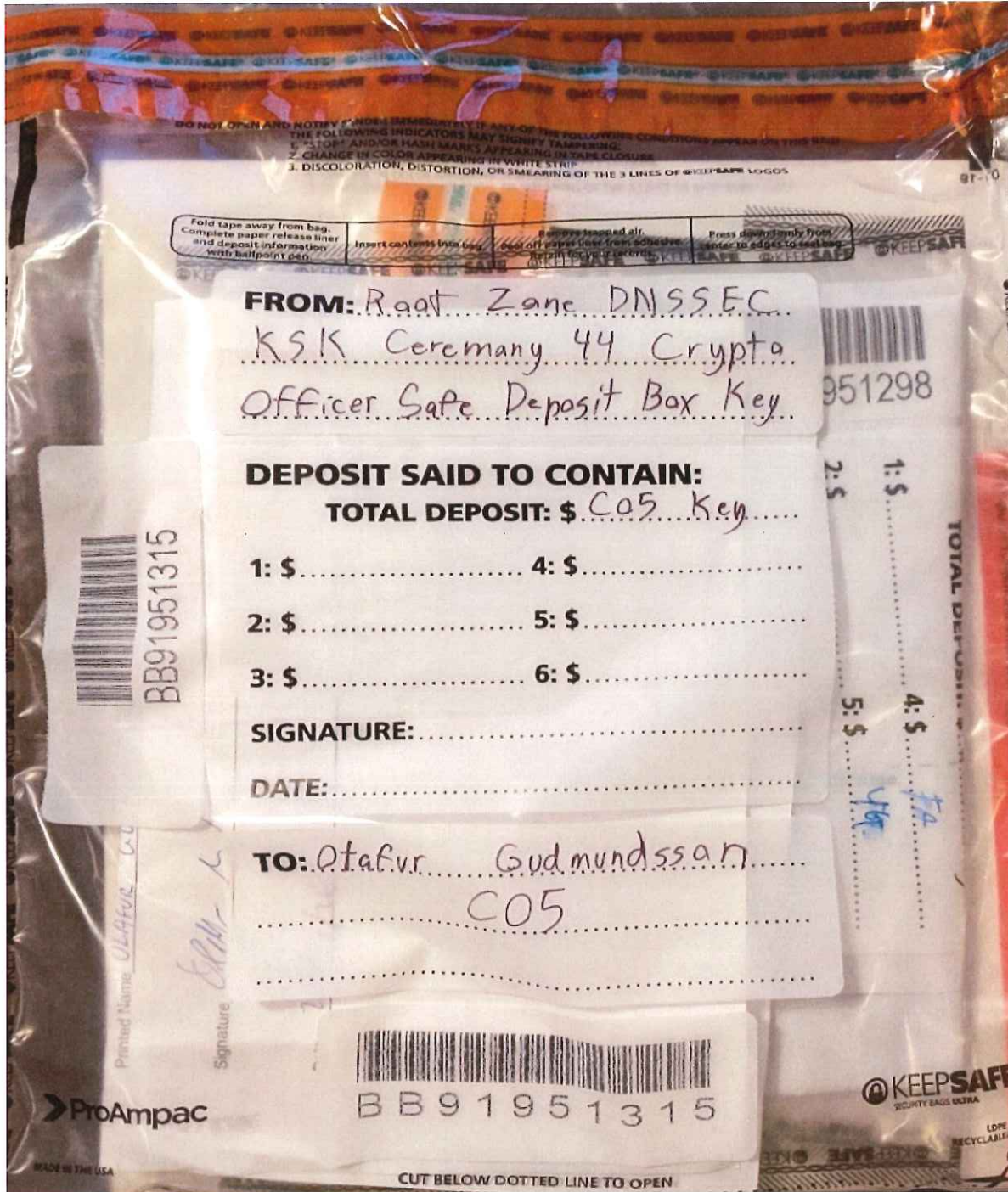
Appendix F: CO4 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO4 Carlos Martinez** Safe Deposit Box Key TEB # **BB91951317** dispatched from the CO.



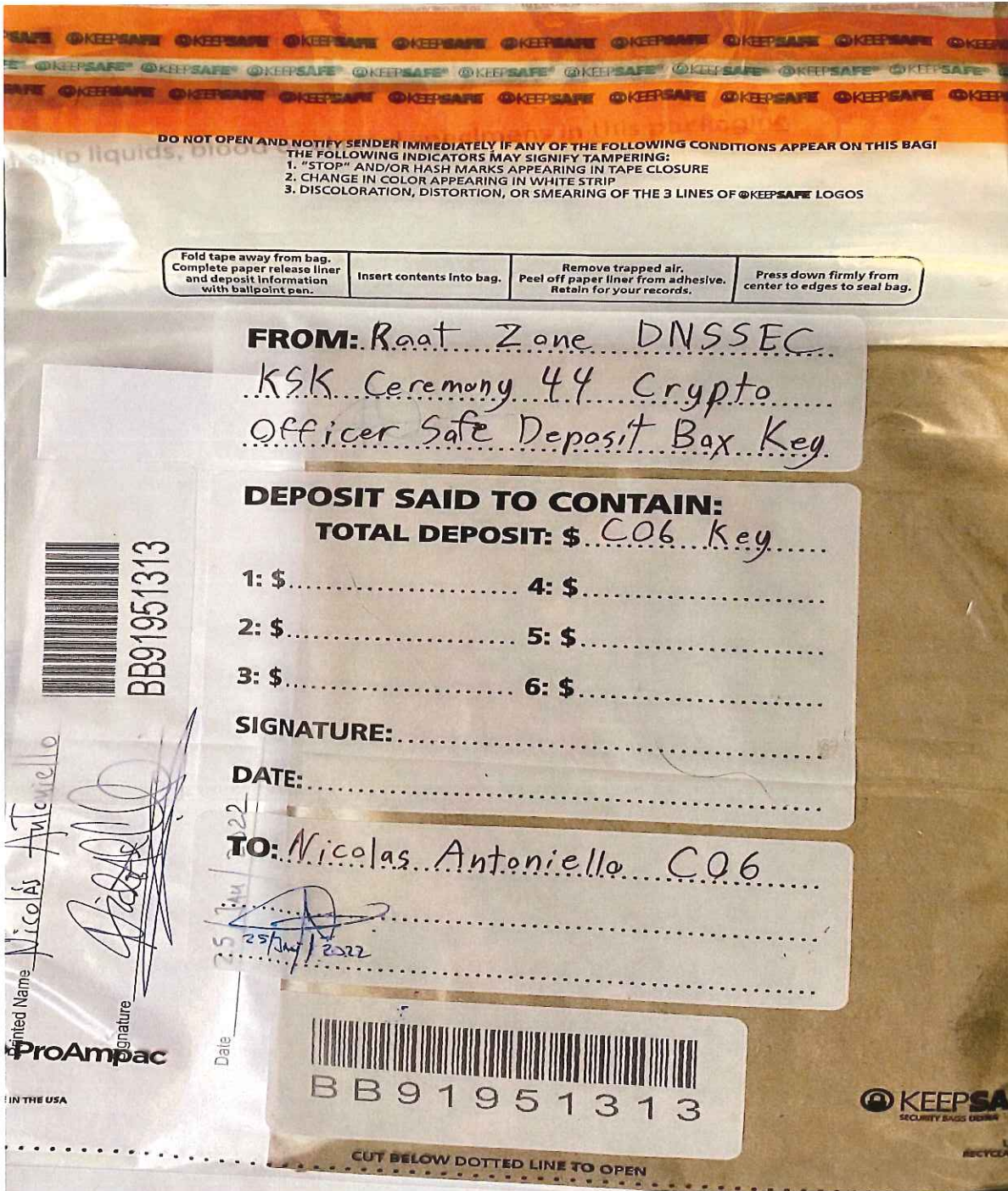
Appendix G: CO5 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO5 Olafur Gudmundsson Safe Deposit Box Key TEB # BB91951315** dispatched from the CO.



Appendix H: CO6 Safe Deposit Box Key Chain of Custody

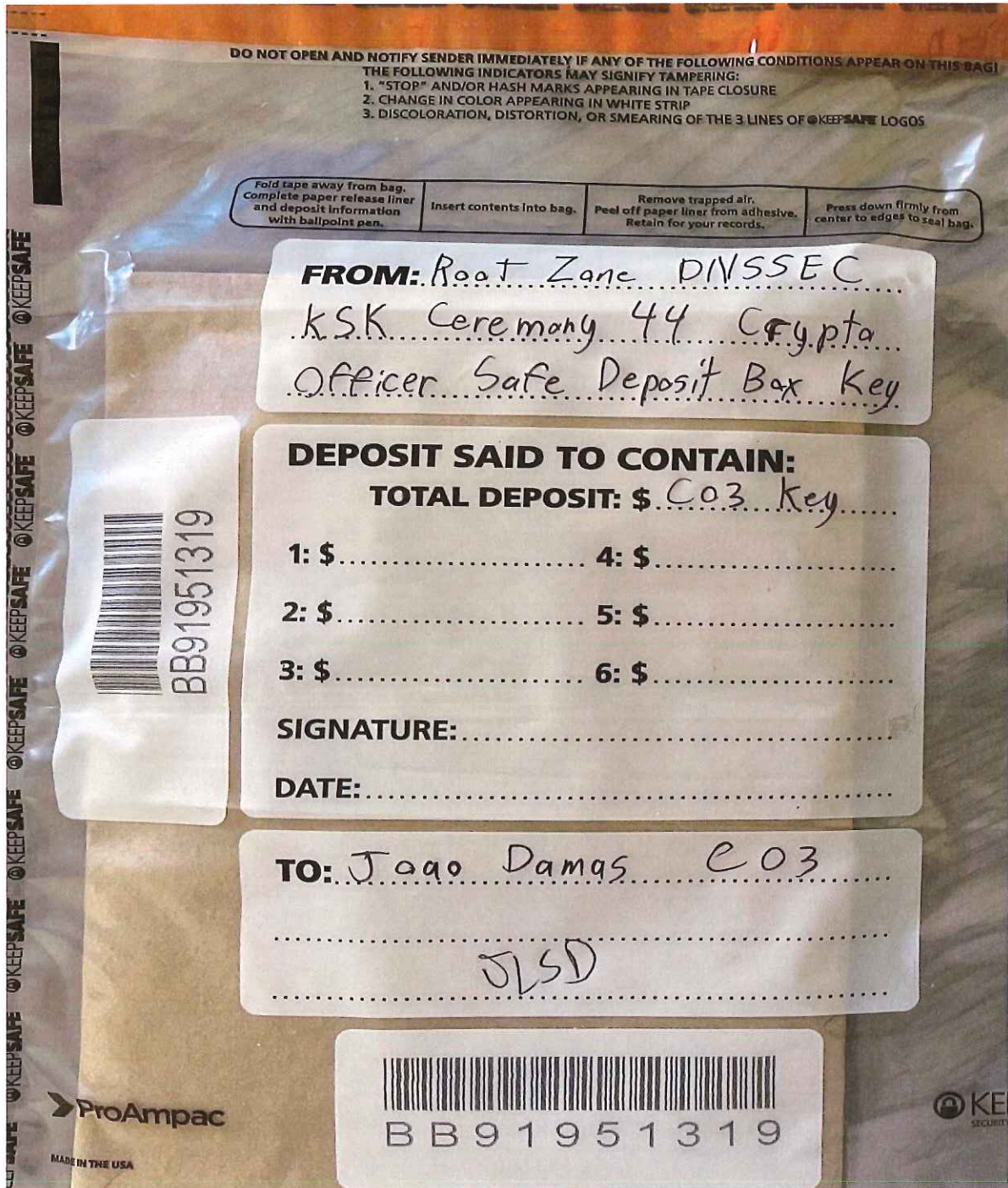
The following photo contains the **CO6 Nicolas Antonielli** Safe Deposit Box Key TEB # **BB91951313** dispatched from the CO.



Appendix I: CO3 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO3 Joao Damas** Safe Deposit Box Key **TEB BB91951319** dispatched from the CO.

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



```
jjenkins@srx> show configuration | no-more
## Last commit: 2021-12-14 19:29:53 UTC by root
version 19.4R3-S1.3;
system {
  host-name srx;
  root-authentication {
    encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
  }
  login {
    user bmartin {
      full-name "Brian Martin";
      uid 2005;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user cbarthold {
      full-name "Connor A. Barthold";
      uid 2004;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user dkara {
      full-name "Darren Kara";
      uid 2001;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user jjenkins {
      full-name "Josh Jenkins";
      uid 2007;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user mcirilo {
      full-name "Moises D. Cirilo";
      uid 2006;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user ptudor {
      full-name "Patrick Tudor";
      uid 2000;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user rquinn {
      full-name "Reed Quinn";
      uid 2003;
      class super-user;
      authentication {
        encrypted-password "XXXXXXXXXXXXXXXXXX"; ## SECRET-DATA
      }
    }
    user sfreak {
```



```
uid 2002;
class super-user;
authentication {
    encrypted-password "XXXXXXXXXXXXXXXXXX"; ## 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-rollback 20;
ntp {
    server 129.6.15.28;
    server 129.6.15.29;
}
}
chassis {
    config-button no-rescue no-clear;
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
}
alarm {
    management-ethernet {
        link-down ignore;
    }
}
}
security {
```

```

pki {
  ca-profile root-ca {
    ca-identity "ICANN Root CA";
    revocation-check {
      crl {
        disable on-download-failure;
      }
    }
    administrator {
      email-address "cbo-team@iana.org";
    }
  }
  ca-profile intermediate-ca {
    ca-identity "ICANN SSL CA";
    revocation-check {
      crl {
        disable on-download-failure;
      }
    }
  }
}
ike {
  proposal ike-proposal-KMF {
    authentication-method rsa-signatures;
    dh-group group24;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
  }
  policy ike-policy-KMF {
    proposals ike-proposal-KMF;
    certificate {
      local-certificate ksk-lax;
    }
  }
  gateway Gateway-to-KMF-East {
    ike-policy ike-policy-KMF;
    address 64.124.6.5;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface ge-0/0/15;
    version v2-only;
  }
}
ipsec {
  proposal IPSecProposal {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 7200;
  }
  policy defaultPolicy {
    perfect-forward-secrecy {
      keys group5;
    }
    proposals IPSecProposal;
  }
  vpn vpn-to-KMF-East {
    bind-interface st0.1;
    ike {
      gateway Gateway-to-KMF-East;
      ipsec-policy defaultPolicy;
    }
    establish-tunnels immediately;
  }
}
screen {

```

```

ids-option external-screen {
  icmp {
    ping-death;
  }
  ip {
    source-route-option;
    tear-drop;
  }
  tcp {
    syn-flood {
      alarm-threshold 1024;
      attack-threshold 200;
      source-threshold 1024;
      destination-threshold 2048;
      timeout 20;
    }
    land;
  }
}
}
nat {
  source {
    rule-set internal-to-external {
      from zone [ access guest wifi ];
      to zone untrust;
      rule source-nat-rule {
        match {
          source-address 0.0.0.0/0;
        }
        then {
          source-nat {
            interface;
          }
        }
      }
    }
  }
}
}
policies {
  from-zone access to-zone untrust {
    policy allow-mail {
      match {
        source-address [ ACC ACS EVM IMS ];
        destination-address icann;
        application junos-smtp;
      }
      then {
        permit;
        log {
          session-close;
        }
      }
    }
  }
  policy allow-dns {
    match {
      source-address [ ACC ACS EVM IMS ];
      destination-address [ icann-dns google-dns ];
      application [ junos-dns-udp junos-dns-tcp ];
    }
    then {
      permit;
      log {
        session-close;
      }
    }
  }
}
}

```

```

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

```

```

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

```

```

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

```

```

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

```

```

interfaces {
  ge-0/0/15.0 {
    host-inbound-traffic {
      system-services {
        ping;
      }
    }
  }
}
security-zone video {
  address-book {
    address kmf_west_video 10.4.28.128/26;
    address VSS 10.4.28.150/32;
    address C1 10.4.28.151/32;
    address C2 10.4.28.152/32;
    address C3 10.4.28.153/32;
    address-set cameras {
      address C1;
      address C2;
      address C3;
    }
  }
  interfaces {
    irb.1 {
      host-inbound-traffic {
        system-services {
          ping;
        }
      }
    }
  }
}
security-zone guest {
  address-book {
    address STR 10.4.28.20/32;
    address VCC 10.4.28.22/32;
    address kmf_west_guest 10.4.28.0/25;
  }
  interfaces {
    irb.2 {
      host-inbound-traffic {
        system-services {
          ping;
        }
      }
    }
  }
}
security-zone ipsec {
  address-book {
    address kmf_east_access 10.4.29.192/26;
    address kmf_east_video 10.4.29.128/26;
    address kmf_east_acs 10.4.29.204/32;
    address kmf_east_acc 10.4.29.202/32;
    address kmf_east_idp 10.4.29.201/32;
    address kmf_east_evm 10.4.29.200/32;
    address kmf_east_ims 10.4.29.203/32;
    address kmf_east_E1 10.4.29.210/32;
    address kmf_east_E2 10.4.29.211/32;
    address kmf_east_E3 10.4.29.212/32;
    address kmf_east_E4 10.4.29.213/32;
    address kmf_east_vss 10.4.29.150/32;
    address kmf_east_C1 10.4.29.151/32;
    address kmf_east_C2 10.4.29.152/32;
    address kmf_east_C3 10.4.29.153/32;
  }
}

```



```

}
interfaces {
  st0.1 {
    host-inbound-traffic {
      system-services {
        ping;
        ike;
      }
    }
  }
}
}
security-zone wifi {
  address-book {
    address kmf_west_wifi 10.100.1.0/24;
  }
  interfaces {
    irb.3 {
      host-inbound-traffic {
        system-services {
          ping;
        }
      }
    }
  }
}
}
}
interfaces {
  ge-0/0/6 {
    ether-options {
      802.3ad ae0;
    }
  }
  ge-0/0/7 {
    ether-options {
      802.3ad ae0;
    }
  }
  ge-0/0/15 {
    unit 0 {
      family inet {
        address 192.0.35.202/26;
      }
    }
  }
  ae0 {
    aggregated-ether-options {
      lacp {
        active;
      }
    }
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members [ vlan-access vlan-guest vlan-video vlan-wifi ];
        }
      }
    }
  }
}
}
}
irb {
  unit 0 {
    description "access vlan";
    family inet {
      address 10.4.28.193/26;
    }
  }
}
}

```

```

    }
  }
  unit 1 {
    description "video vlan";
    family inet {
      address 10.4.28.129/26;
    }
  }
  unit 2 {
    description "guest vlan";
    family inet {
      address 10.4.28.1/25;
    }
  }
  unit 3 {
    description "wifi vlan";
    family inet {
      address 10.100.1.1/24;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      filter {
        input route-engine-filter;
      }
    }
  }
}
st0 {
  unit 1 {
    description "IPSec KMF-West";
    family inet;
  }
}
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; }}
}
```