Root DNSSEC KSK Ceremony 53-1

Thursday 25 April 2024

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

This ceremony is executed in accordance with the DNSSEC Practice Statement for the Root Zone KSK Operator 7th Edition (2024-03-15)

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
MC	= Master of Ceremonies	**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	**STM**	= Secure Transport Mode
SW	= Staff Witness	**TCR**	= Trusted Community Representative		
TEB	= Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20)				

Participants

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

Title / Roles	Printed Name	Signature	Date	Time
CA	David Huberman / ICANN			
IW	Andy Newton / ICANN			
SSC1	Fernanda Iunes / ICANN			
SSC2	Hope Shafer / ICANN			
CO1	Frederico Neves			
CO2	Pia Gruvö			
CO3	Ondrej Filip			
CO4	Robert Seastrom			
CO5	Nomsa Mwayenga			
CO6	Hugo Salgado			
CO7	Dileepa Lathsara			
RKSH1	Sebastian Castro			
RKSH2	Ondřej Surý			
RKSH3	Kristian Ørmen		2024 Apr 25	22:13
RKSH4	Jiankang Yao			
RKSH5	Bevil Wooding			
RKSH6	John Curran			
RKSH7	Dave Lawrence			
RZM	Trevor Davis / Verisign			
AUD	Melanie Chen / RSM			
AUD	Grant An / RSM			
SA	Darren Kara / 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 begins recording with the audit cameras shortly before the ceremony begins
- 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 HSMs 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 active
- 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
- Explain the purpose of the ceremony along with a high-level list of tasks to be completed

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

- Safe #1 containing all equipment: HSMs, laptops, OS media, etc
- Safe #2 containing all credentials: Crypto Officer credentials are required to operate HSMs

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1.1	CA confirms with SA that all audit cameras are recording and online video streaming is active.	_M_	17:60
1.2	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.	_Mn_	17:02
1.3	CA asks that any first-time ceremony participants in the room introduce themselves.	_M_	17:03

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
1.4	CA reviews emergency evacuation procedures with onsite participants.	_M_	17:03
1.5	CA explains the use of personal electronic devices during the ceremony.	_M_	17:03
1.6	CA summarizes the purpose of the ceremony.	_M_	17:06

Verify the Time and Date

Step	Activity	Initials	Time
1.7	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: _2024/04/25 17:06:22_ Note: All entries into this script or any logs should follow this common source of time.	_M_	17:06

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1.8	CA transports the guard key and flashlight, and with IW escorts SSC2 and the COs into Tier 5 (Safe Room.)	/M	17:08
1.9	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.**	/Mu	17:09
1.10	Perform the following steps to update the safe log: a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies the entry, then initials it.	/Mu	17:11

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

Step	Activity	Initials	Time
1.11	COs perform the following steps sequentially to access the listed TEBs: a) CO announces their box number, then CA operates the guard key in that box's lower lock with the key blade facing downward. b) CO operates their tenant key in that box's upper lock with the key blade facing upward, then opens the safe deposit box. c) CO verifies the box's integrity, then removes the TEBs. d) CO reads aloud the TEB numbers, verifies integrity of TEBs, then presents them to the audit camera above. e) CO performs the actions specified below, locks their safe deposit box, and removes their key. f) CO writes the date and time, then signs the safe log. g) IW verifies the completed safe log entries, then initials them. h) CA locks the safe deposit box, then removes the guard key. **CO1: Frederico Neves - Box # 1239** **Set # 1 TEB # BB02638669** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02638534** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO2: Pia Gruvö - Box # 1264** **Set # 1 TEB # BB02638668** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02639498** (Retain) Last Verified: KSK Ceremony 47 2022-11-03 **CO3: Ondrej Filip - Box # 1241** **Set # 1 TEB # BB02639557** (Check and Return) Last Verified: KSK Ceremony 45 2022-05-12 **Set # 2 TEB # BB02638533** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO4: Robert Seastrom - Box # 1243** **Set # 1 TEB # BB02638667** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02639551** (Retain) Last Verified: KSK Ceremony 45 2022-05-12 **CO5: Nomsa Mwayenga - Box # 1262** **Set # 1 TEB # BB02638666** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02638665** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **CO6: Hugo Salgado - Box # 1242** **Set # 1 TEB # BB02638664** (Check and Return) Last Verified: KSK Ceremony 51 2023-11-30 **Set # 2 TEB # BB02638530** (Check and Return) Last Verified: KSK Ceremony 49 2023-04-27 **CO7: Dileepa Lathsara - Box # 1263** **Set # 1 TEB # BB02639495** (Check and Return) Last Verified: KSK Ceremony 47 2022-11-03 **Set # 2 TEB # BB02638529** (Retain) Last Verified: KSK Ceremony 49 2023-04-27 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	_MW_	17:27

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1.12	Once all safe deposit boxes are closed and locked, SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.	*M*	17:27
1.13	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, then 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 adjacent to the Tier 5 (Safe Room) exit door is off.	*M*	17:26
1.14	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) with TEBs, returning to Tier 4 (Key Ceremony Room).	*M*	17:27

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
1.15	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)	*M*	17:30
1.16	SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.	*M*	17:31

1.17	Perform the following steps to update 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.
		M	17:32

Access Equipment in Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
1.18	CA performs the indicated action for each item listed below with the following steps: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud the TEB number, verify its integrity, then present it to the audit camera above. c) Place the equipment TEB on the cart as specified in the list below. d) Write the date and time, then sign the safe log. e) IW verifies the completed safe log entries, then initials them. **HSM5E: TEB # BB51184250 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **HSM6E: TEB # BB51184243 (Stored for Backup Purposes)** Last Verified: KSK Ceremony 49 2023-04-27 **HSM7E: TEB # BB51184251 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **HSM8E: TEB # BB51184252 (Check and Return)** Last Verified: KSK Ceremony 51 2023-11-30 **Laptop3: TEB # BB97448418 (Place on Cart)** Last Verified: KSK Ceremony 49 2023-04-27 **Laptop4: TEB # BB81420078 (Check and Return)** Last Verified: KSK Ceremony 51 2023-11-30 **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 **KSK-2017: TEB # BB02638662 (Check and Return)** Last Verified: KSK Ceremony 51 2023-11-30 **KSK-2023: TEB # BB02638661 (Place on Cart)** Last Verified: KSK Ceremony 51 2023-11-30 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes. The shelves in the equipment safe can slide in and out for ease of use.	_(signed)_	17:41

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

Step	Activity	Initials	Time
1.19	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry then initials it.	_(signed)_	17:41
1.20	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, then 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 adjacent to the Tier 5 (Safe Room) exit door is off.	_(signed)_	17:42
1.21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	_(signed)_	17:42

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 2 Step(s): 2.4 2.5 Page(s): 10 Date and time of the exception: 2024-04-25 17:52 Note: IW describes the exception(s) and action(s) below.	*MU*	17:54

Laptop would not boot. CA with assistance of Aaron accessed the laptop BIOS and accepted the date and time. The laptop then booted successfully.

Act 2: Introduce New OS Media

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

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

Laptop3 Setup

Step	Activity	Initials	Time
2.1	CA performs the following steps to prepare each item listed below: a) Remove the TEB from the cart, then place it on the ceremony table. b) Inspect the 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. **Laptop3: TEB # BB97448418 / Service Tag # J8SVSG2** Last Verified: KSK Ceremony 49 2023-04-27 **OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663** Last Verified: KSK Ceremony 51 2023-11-30 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	*M*	17:46
2.2	CA performs the following steps to confirm that no hard drive and battery are in the laptop: a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty.	*M*	17:47
2.3	CA ensures the **lock switch** on the left side of the listed SD card is slid down to the lock position: **OS media release coen-1.0.0** **Copy # 1**	*M*	17:48
2.4	CA performs the following steps to boot the laptop: a) Connect the external HDMI display cable. b) Connect the power supply. c) Insert the **OS media release coen-1.0.0 Copy # 1**. d) Switch it ON.	*M*	17:50
2.5	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	*M*	17:54

OS Media coen-1.0.0 Checksum Verification

Step	Activity	Initials	Time

2.6	Using the **Commands** terminal window, CA executes the following steps:
	
	a) Verify the byte count of the SD card matches the **OS media release coen-1.0.0** ISO size **375431168** by running the following command:
	`df -B1 /dev/sda`
	
	b) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sda | sha2wordlist`
	
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.
	
	SHA-256 hash:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1
		[signature]	17:56

OS Media coen-1.1.0 Acceptance Test

Step	Activity	Initials	Time
2.7	CA connects the external SD card reader to a USB port in the laptop.	_Au_	17:57
2.8	CA ensures the **lock switch** on the left side of the SD card is slid down to the lock position.	_Au_	17:58

2.9	CA inserts the new **OS media release coen-1.1.0** SD card into the external SD card reader, then using the **Commands** terminal window performs the following steps:
	Note: The SD card should be inserted upside-down with the writing on top of the SD card reader visible.
	
	a) Confirm the external SD card ID of /dev/sdb by executing:
	`lsblk`
	b) Mount the external SD card by executing:
	`mount /dev/sdb /mnt`
	c) Verify the byte count of the SD card matches the **OS media release coen-1.1.0** ISO size **602406912** by running the following command:
	`df -B1 /dev/sdb`
	d) Calculate the SHA-256 hash by executing:
	`head -c 602406912 /dev/sdb
		sha2wordlist`
		e) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash.
		Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script.
		f) Unmount the external SD card by executing:
		`umount /dev/sdb`
		
		SHA-256 hash:
		2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8
		PGP Words:
		blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous
		
		Note: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1
			_Au_	18:a

2.10	CA removes the new OS media SD card, then places it on the ceremony table. Note: The tested OS media must be placed on the ceremony table where it is visible to the audit camera and the participants	_Au_	18:01
2.11	CA repeats steps **2.8** to **2.10** for the 2nd copy of the new **OS media release coen-1.1.0** SD card.	_Au_	18:04
2.12	CA disconnects the external SD card reader from the laptop.	_Au_	18:04

Retire Previous OS Media coen-1.0.0

Step	Activity	Initials	Time
2.13	CA performs the following steps to switch OFF the laptop and remove the OS media: a) Remove the OS media from the laptop, and place it in its case. b) Power **OFF** the laptop by pressing the power button. c) Disconnect all connections from the laptop. d) Discard all copies of the **OS media release coen-1.0.0**.	_Au_	18:06

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 3 Step(s): 3.3 Page(s): 13 Date and time of the exception: 2024-04-25 18:13 Note: IW describes the exception(s) and action(s) below.	_Mu_	1815

Laptop did not boot into OS. CA booted laptop into BIOS, observed the time and date, exited the BIOS. The laptop then booted into the OS.

Act 3: Equipment Setup

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

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

Laptop3 Setup

Step	Activity	Initials	Time
3.1	CA performs the following steps to prepare each item listed below: a) Remove the TEB from the cart, then place it on the ceremony table. b) Inspect the 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. **HSM7E: TEB # BB51184251 / Serial # H2110009** Last Verified: KSK Ceremony 51 2023-11-30 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	*Au*	18:09
3.2	CA ensures the **lock switch** on the left side of the listed SD card is slid down to the lock position: **OS media release coen-1.1.0** **Copy # 1**	*Au*	18:10
3.3	CA performs the following steps to boot the laptop: a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into a USB port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Insert the **OS media release coen-1.1.0 Copy # 1**. f) Switch it ON.	*Au*	18:15
3.4	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the **View** menu and select **Zoom In** or **Zoom Out** To change the resolution of each screen: Go to **Applications > Settings > Display**	*Au*	18:15

OS Media coen-1.1.0 Checksum Verification

Step	Activity	Initials	Time
3.5	Using the **Commands** terminal window, CA executes the following steps: a) Verify the byte count of the SD card matches the **OS media release coen-1.1.0** ISO size **602406912** by running the following command: `df -B1 /dev/sda` b) Calculate the SHA-256 hash by executing: `head -c 602406912 /dev/sda	sha2wordlist` c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script. SHA-256 hash: 2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8 PGP Words: blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous Note: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1	_M_	18:17

Printer Setup

Step	Activity	Initials	Time
3.6	CA confirms that the printer is switched ON:	_M_	18:17
3.7	Using the **Commands** terminal window, CA executes the command below to configure the printer and print a test page: `configure-printer`	_M_	18:18

Date Setup

Step	Activity	Initials	Time
3.8	Using the **Commands** terminal window, CA executes the command below to verify the date/time reasonably matches the ceremony clock. `date` If the date/time do not match, perform the following steps: a) Execute `date -s "20240425 HH:MM:SS"` to set the time. where HH is two-digit hour, MM is two-digit minutes and SS is two-digit seconds. b) Execute `date` to confirm the date/time matches the clock.	_M_	18:19

Connect the Ceremony 51 HSMFD

Step	Activity	Initials	Time
3.9	CA plugs the **Ceremony 51 HSMFD** into a USB slot, then performs the steps below: a) Wait for the file system window to appear. b) Display the HSMFD contents to all participants. c) Close the file system window.	_Mu_	18:20
3.10	Using the **Commands** terminal window, CA executes the command below to calculate the SHA-256 hash of the HSMFD: `hsmfd-hash -c` CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script. HSMFD SHA-256 HASH 2023/11/30 # find -P /media/HSMFD/ -type f -print0 | LC_COLLATE=POSIX sort -z | xargs -0 cat | sha2wordlist SHA-256: 5c9ad14c8628b3176a841379f9cf1d7c37213a9669b69d6dabecf77292e53c37 PGP Words: escape newsletter stairway disbelief necklace cellulose scallion bookseller Geigher Jupiter Aztec inertia waffle Saturday Belfast informant clamshell Camelot cleanup lettrhead gazelle potato quadrant hazardous rhythm unicorn virus holiness physique travesty cobra consensus IW confirms that the result matches the SHA-256 hash of the HSMFD using the printed HSMFD hash from the Ceremony 51 OS Media bundle.	_Mu_	18:22

Distribute Unused Ceremony 51 HSMFD

Step	Activity	Initials	Time
3.11	CA gives the unused **Ceremony 51 HSMFD** and the sheet of paper with the printed HSMFD hash to RKOS.	_Mu_	18:22
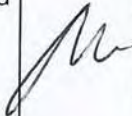
Start the Terminal Session Logging

Step	Activity	Initials	Time
3.12	Using the **Commands** terminal window, CA executes the command below to change the working directory to HSMFD: `cd /media/HSMFD`	_Mu_	18:23
3.13	Using the **Commands** terminal window, CA executes the command below to log activities of the terminal window: `script script-20240425.log`	_Mu_	18:23

Start the HSM Output Logging

Step	Activity	Initials	Time

3.14	Using the **HSM Output** terminal window, CA performs the following steps to capture the activity logs of the HSM:
	 a) Change the working directory to HSMFD by executing:
	 `cd /media/HSMFD`
	 b) Set the serial port baud rate by executing:
	 `stty -F /dev/ttyUSB0 115200`
	 c) Start logging the serial output by executing:
	 `ttyaudit /dev/ttyUSB0`
	
	 Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.
		_Mu_	18:24

Power ON HSM7E (Tier 7)

Step	Activity	Initials	Time
3.15	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM7E**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. **Note: Status information should appear in the HSM output terminal window.** d) Scroll up on the terminal window while IW verifies the displayed HSM serial number on the screen reads **H2110009**. e) Scroll down to the end of the terminal window. **HSM7E: Serial # H2110009** Note: The date and time on the HSM is not used as a reference for logging and timestamp.	_M_	18:25

Act 4: Activate HSM7E (Tier 7) and Generate Signatures

Using the ksr signer application, the CA uses the Key Signing Requests (KSRs) in conjunction with the HSM to generate the Signed Key Responses (SKRs) by performing the steps below:

- The CA activates the HSM using the Crypto Officers' credentials
- After connectivity is confirmed, the flash drive containing the KSRs is inserted into the laptop
- The ksr signer application uses the private key stored in the HSM to generate the SKRs containing the digital signatures of the ZSK slated for future Root Zone signing
- The CA prints the signer log, backs up the newly generated SKRs, then deactivates the HSM

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
4.1	The CA calls each of the COs listed below sequentially to perform the following steps: a) CO reads aloud the TEB number, then CA inspects it for tamper evidence while the IW verifies its "last verified" information using the specified previous ceremony script. b) CO and CA open the TEB, then the CA removes the credential case to perform the action specified below. **CO2: Pia Gruvö** **Set # 2 TEB # BB02639498** (CO places cards on their designated card holders) Last Verified: KSK Ceremony 47 2022-11-03 **CO4: Robert Seastrom** **Set # 2 TEB # BB02639551** (CO places cards on their designated card holders) Last Verified: KSK Ceremony 45 2022-05-12 **CO7: Dileepa Lathsara** **Set # 2 TEB # BB02638529** (CO places cards on their designated card holders) Last Verified: KSK Ceremony 49 2023-04-27 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	_(signature)_	18:31

Enable/Activate HSM7E (Tier 7)

Step	Activity	Initials	Time
	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert a randomly selected 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.		
4.2	Confirm the **"READY"** LED on the **HSM** is **ON**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st OP card __4__ of 7 2nd OP card __7__ of 7 3rd OP card __2__ of 7 Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.	_Mw_	18:33

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
4.3	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	_Mw_	18:34

4.4	CA performs the following steps to test the network connectivity between laptop and HSM:
	a) Select the **Commands** terminal window
	b) Test connectivity by executing:
	`ping hsm`
	c) Wait for responses, then exit by pressing:
	`Ctrl + C`
		_Mw_	18:34

Insert the KSRFD

Step	Activity	Initials	Time
4.5	CA plugs the **KSRFD** into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window. Note: The KSRFD was transferred to the facility by the RKOS. It contains 1 KSR.	_Mw_	18:35

Execute the KSR Signer for KSR 2024 Q3

Step	Activity	Initials	Time
4.6	Using the **Commands** terminal window, the CA executes the command below to change the working directory: `cd /media/KSRFD/KSK53-1/`	_Mw_	18:36
4.7	Using the **Commands** terminal window, the CA executes the command below to sign the KSR file: `kskm-ksrsigner`	_Mw_	18:36

25 April 2024

The SHA256 hash of the 2024 Q3 KSR file is:

ksr-root-2024-q3-0.xml:

51ffea38b7a12484129055c570e17a366408e1b5bff642463e13
b098b254f705

The PGP wordlist for the hash above is:

PGP Words: drunken Yucatan Trojan consulting seabird
outfielder bluebird Jupiter atlas millionaire edict
resistor guidance tolerance keyboard congregate
flytrap antenna tempest positive slingshot vocalist
crowfoot detergent concert barbecue ruffled narrative
sawdust equation virus almighty

Attested on behalf of VeriSign by:

Trevor Davis
Senior Manager
Cryptographic Business Operations
VeriSign, Inc.

February 12, 2024

To Whom It May Concern:

This is a letter of Verification of Employment for Trevor Davis. VeriSign, Inc. ("Verisign") has employed Trevor Davis full-time/40 hours per week since September 29, 2014, currently as a Senior Manager - Engineering in Verisign's Production Operations department.

Should you have further questions, please contact me at dcarney@verisign.com or (571) 328-8057.

Sincerely,

X ~Dave Carney~ February 12, 2024

Dave Carney
Sr. HR Specialist

Loaded configuration from file ksrsigner.yaml SHA-256 962c515dd68bee5380fd50e2ec98dfe0c971f6634c3b211
e9444a3b2ffe179f9 WORDS prefer Chicago drunken filament stockman Medusa tycoon enterprise merit Wyomi
ng drumbeat tomorrow tumor narrative talon tobacco spearhead hideaway village Galveston drainage coun
cilman blackjack Burlington Pluto designing reform pioneer Zulu tolerance jawbone Waterloo
Configuration validated
Loaded SKR from file skr-root-2024-q2-0.xml SHA-256 d6b445c09306a9cb44d99cb77321085b53b1fd68b6d73d488
f958571f631dd62 WORDS stockman politeness crusade recipe playhouse amulet revenge revival crumpled su
pportive python processor hockey Camelot aimless exodus dwelling photograph willow gravity Scotland s
tethoscope commence dictator payday Montana music hideaway village company swelter gadgetry
Previous SKR:

#	Inception	Expiration	ZSK Tags	KSK(CKA_LABEL)
1	2024-04-01T00:00:00	2024-04-22T00:00:00	30903,5613	20326(Klajeyz)/S
2	2024-04-11T00:00:00	2024-05-02T00:00:00	5613	20326(Klajeyz)/S
3	2024-04-21T00:00:00	2024-05-12T00:00:00	5613	20326(Klajeyz)/S
4	2024-05-01T00:00:00	2024-05-22T00:00:00	5613	20326(Klajeyz)/S
5	2024-05-11T00:00:00	2024-06-01T00:00:00	5613	20326(Klajeyz)/S
6	2024-05-21T00:00:00	2024-06-11T00:00:00	5613	20326(Klajeyz)/S
7	2024-05-31T00:00:00	2024-06-21T00:00:00	5613	20326(Klajeyz)/S
8	2024-06-10T00:00:00	2024-07-01T00:00:00	5613	20326(Klajeyz)/S
9	2024-06-20T00:00:00	2024-07-11T00:00:00	20038,5613	20326(Klajeyz)/S

Loaded KSR from file ksr-root-2024-q3-0.xml SHA-256 51ffea38b7a12484129055c570e17a366408e1b5bff642463
e13b098b254f705 WORDS drunken Yucatan Trojan consulting seabird outfielder bluebird Jupiter atlas mil
lionaire edict resistor guidance tolerance keyboard congregate flytrap antenna tempest positive sling
shot vocalist crowfoot detergent concert barbecue ruffled narrative sawdust equation virus almighty
Validating KSR using request policy:
　　_dataclass_placeholder: None
　　acceptable_domains: ['.']
　　approved_algorithms: ['RSASHA256']
　　check_bundle_intervals: True
　　check_bundle_overlap: True
　　check_chain_keys: True
　　check_chain_keys_in_hsm: True
　　check_chain_overlap: True
　　check_cycle_length: True
　　check_keys_match_ksk_operator_policy: True
　　check_keys_publish_safety: True
　　check_keys_retire_safety: True
　　dns_ttl: 172800
　　enable_unsupported_ecdsa: False
　　keys_match_zsk_policy: True
　　max_bundle_interval: 11 days, 0:00:00
　　max_cycle_inception_length: 81 days, 0:00:00
　　min_bundle_interval: 9 days, 0:00:00
　　min_cycle_inception_length: 79 days, 0:00:00
　　num_bundles: 9
　　num_different_keys_in_all_bundles: 3
　　num_keys_per_bundle: [2, 1, 1, 1, 1, 1, 1, 1, 2]
　　rsa_approved_exponents: [65537]
　　rsa_approved_key_sizes: [2048]
　　rsa_exponent_match_zsk_policy: True
　　signature_algorithms_match_zsk_policy: True
　　signature_check_expire_horizon: True
　　signature_horizon_days: 180
　　signature_validity_match_zsk_policy: True
　　validate_signatures: True
KSR-DOMAIN: Verified domain '.'
KSR-ID: Will be checked later, when SKR is available
KSR-BUNDLE-UNIQUE: All 9 bundles have unique ids
KSR-BUNDLE-KEYS: All 3 unique keys in the bundles accepted by policy
KSR-BUNDLE-POP: All 9 bundles contain proof-of-possession
KSR-BUNDLE-COUNT: Number of bundles (9) accepted
KSR-BUNDLE-CYCLE-DURATION: The cycle length is in accordance with the KSK operator policy
KSR-POLICY-KEYS: Validated number of keys per bundle, and for all bundles
KSR-POLICY-ALG: All 1 ZSK operator signature algorithms accepted by policy
KSR-POLICY-SIG-OVERLAP: All bundles overlap in accordance with the stated ZSK operator policy
KSR-POLICY-SIG-VALIDITY: All 9 bundles have 21 days <= validity >= 21 days
KSR-POLICY-SIG-HORIZON: All signatures expire in less than 180 days
KSR-POLICY-BUNDLE-INTERVALS: All bundles intervals in accordance with the KSK operator policy
Request:

#	Inception	Expiration	ZSK Tags	KSK(CKA_LABEL)
1	2024-07-01T00:00:00	2024-07-22T00:00:00	20038,5613	
2	2024-07-11T00:00:00	2024-08-01T00:00:00	20038	
3	2024-07-21T00:00:00	2024-08-11T00:00:00	20038	
4	2024-07-31T00:00:00	2024-08-21T00:00:00	20038	
5	2024-08-10T00:00:00	2024-08-31T00:00:00	20038	

```
6   2024-08-20T00:00:00 2024-09-10T00:00:00   20038
7   2024-08-30T00:00:00 2024-09-20T00:00:00   20038
8   2024-09-09T00:00:00 2024-09-30T00:00:00   20038
9   2024-09-19T00:00:00 2024-10-10T00:00:00   20038,61050
```

Initializing PKCS#11 module aep using /opt/Keyper/PKCS11Provider/pkcs11.linux_gcc_4_1_2_glibc_2_5_x86
_64.so.5.02
HSM First slot: ICANNKSK
HSM ManufacturerID: Ultra Electronics AEP Networks
HSM Model: Keyper 9860-2
HSM Serial: H2110009
Checking coherence between SKR(n-1) and this KSR
KSR-CHAIN-KEYS: The last keys in SKR(n-1) matches the first keys in this KSR
KSR-CHAIN-OVERLAP: Overlap with last bundle in SKR(n-1) 10 days is in accordance with the KSR policy
KSR-CHAIN-KEYS: All 1 signatures in the last bundle of the last SKR were made with keys present in th
e HSM(s)
KSR-POLICY-SAFETY: PublishSafety validated
KSR-POLICY-SAFETY: RetireSafety validated
Generated SKR:

```
#   Inception            Expiration            ZSK Tags      KSK(CKA_LABEL)
1   2024-07-01T00:00:00 2024-07-22T00:00:00   20038,5613    20326(Klajeyz)/S
2   2024-07-11T00:00:00 2024-08-01T00:00:00   20038         20326(Klajeyz)/S
3   2024-07-21T00:00:00 2024-08-11T00:00:00   20038         20326(Klajeyz)/S
4   2024-07-31T00:00:00 2024-08-21T00:00:00   20038         20326(Klajeyz)/S
5   2024-08-10T00:00:00 2024-08-31T00:00:00   20038         20326(Klajeyz)/S
6   2024-08-20T00:00:00 2024-09-10T00:00:00   20038         20326(Klajeyz)/S
7   2024-08-30T00:00:00 2024-09-20T00:00:00   20038         20326(Klajeyz)/S
8   2024-09-09T00:00:00 2024-09-30T00:00:00   20038         20326(Klajeyz)/S
9   2024-09-19T00:00:00 2024-10-10T00:00:00   20038,61050   20326(Klajeyz)/S
```

Wrote SKR to file skr-root-2024-q3-0.xml SHA-256 bb9a5163436ff368220e4c7e7b0f69725b9f6484a6dd36780a1f
5e482a992279 WORDS shamrock newsletter drunken Galveston crucial hemisphere upset gravity blockade At
lantic drainage insurgent kickoff atmosphere gazelle holiness erase opulent flytrap Jupiter rematch t
ambourine Christmas indigo allow businessman eyeglass dictator brickyard nebula blockade inertia

Verify the KSR Hash for KSR 2024 Q3

Step	Activity	Initials	Time
4.8	When the hash of the KSR is displayed in the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification **off camera** for the purpose of authentication while maintaining privacy. Note: If the RZM representative is not physically present in the room, write the representative's name and *"Remote Participant"* next to the name on the signature line. b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line: Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS in advance to be included in the final annotated script and audit bundle. Trevor Davis _____ c) The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.	*[initials]*	18:37
4.9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks **"are there any objections?"**	*[initials]*	18:39
4.10	CA enters **Yes** in response to **"Sign KSR?"** to complete the KSR signing operation. The SKR is located at: `/media/KSRFD/KSK53-1/skr-root-2024-q3-0.xml`	*[initials]*	18:39

Print Copies of the KSR Signer Log(s)

Step	Activity	Initials	Time
4.11	Using the **Commands** terminal window, the CA executes the commands below to print the KSR Signer log: a) `printlog kskm-ksrsigner-202404*.log X` Note: Replace "X" with the quantity of copies needed for the participants.	*[initials]*	18:42
4.12	IW attaches a copy of the required ksr signer log to their script.	*[initials]*	18:42
4.13	Using the **Commands** terminal window, the CA executes the command below to change the working directory: `cd /media/HSMFD`	*[initials]*	18:42

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 4 Step(s): 4,14 Page(s): 20 Date and time of the exception: 2024-04-25 6:47 Note: IW describes the exception(s) and action(s) below.	*ML*	18:50

The CA executed the copy command without the trailing period resulting into a copy of the files in a subdirectory. After executing the copy command with the trailing period character, the CA executed the necessary steps to remove the accidentally created files under consultation of the Linux experts present in the room.

Copy the Newly Generated SKR(s)

Step	Activity	Initials	Time

4.14	CA executes the following commands using the terminal window:
	a) List the contents of the KSRFD by executing:
	`ls -ltrR /media/KSRFD`
	b) Copy the contents of the KSRFD to the HSMFD by executing:
	`cp -pR /media/KSRFD/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD by executing:
	`ls -ltrR`
	d) Verify it has been copied successfully by executing:
	`diff -qr /media/HSMFD/KSK53-1/ /media/KSRFD/KSK53-1/`
	e) Unmount the KSRFD by executing:
	`umount /media/KSRFD`
	Note: When executing a diff command, a return of no output indicates a match.
		(initialed)	18:50

4.15	CA removes the **KSRFD** containing the SKR files, then gives it to the RZM representative. **Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.**	*(initialed)*	18:51

Disable/Deactivate HSM7E (Tier 7)

Step	Activity	Initials	Time
4.16	CA deactivates the HSM by performing the following steps: **Note: CA will use OP cards not previously utilized in this ceremony if available.** a) CA selects the **HSM Output** terminal window. b) Utilize the HSM's keyboard to scroll through the menu using < > c) Select **"2.Set Offline"**, press **ENT** to confirm. d) When **"Set Offline?"** is displayed, press **ENT** to confirm. e) When **"Insert Card OP #X?"** is displayed, insert a randomly selected OP card. f) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. g) When **"Remove Card?"** is displayed, remove the OP card. h) Repeat steps **e)** to **g)** for the 2nd and 3rd OP cards. Confirm the **"READY"** LED on the **HSM** is **OFF**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st OP card __7__ of 7 2nd OP card __2__ of 7 3rd OP card __4__ of 7 **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **Use credentials that haven't been used previously during this ceremony when possible.** **For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.**	*(initialed)*	18:53

Place HSM7E (Tier 7) into a TEB

Step	Activity	Initials	Time
4.17	CA switches the HSM power **OFF**, then disconnects the power, serial, and ethernet connections. Note: DO NOT unplug the cable connections on the laptop.	*(initials)*	18:54
4.18	CA performs the following steps to prepare the HSM for storage: a) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. **HSM7E: TEB # BB51184553 / Serial # H2110009**	*(initials)*	18:56

OS Media coen-1.1.0 Checksum Verification

Step	Activity	Initials	Time
4.19	Using the **Commands** terminal window, CA executes the following steps: a) Verify the byte count of the SD card matches the **OS media release coen-1.1.0** ISO size **602406912** by running the following command: `df -B1 /dev/sda` b) Calculate the SHA-256 hash by executing: `head -c 602406912 /dev/sda	sha2wordlist` c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script. SHA-256 hash: 2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c529390d8 PGP Words: **blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse souvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peachy stupendous** Note 1: The SHA-256 hash of the OS media is being calculated a second time to ensure the contents of the SD card have not been modified during the previous steps. Note 2: The SHA-256 hash of the OS media release coen-1.1.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/53-1	*(initials)*	18:56

Ceremony Break

Step	Activity	Initials	Time
4.20	CA divides the participants who desire a ceremony break into groups and ensures the following: a) Remaining participants are sufficient to maintain dual occupancy guidelines for the ceremony room. b) Audit Cameras are never obstructed. c) Live stream audio is muted until the ceremony resumes. RKOS will escort each group of participants out of the ceremony room for the ceremony break.	_M_	19:13
4.21	Once all of the groups have returned to Tier 4 (Ceremony Room) from the break, CA ensures live stream audio is enabled, all participants are present by performing a roll call, then resumes the ceremony.	_M_	19:14

Act 5: Test and Replace Recovery Key Share Holders' (RKSHs) Storage Master Key (SMK) Cards

The currently-issued Recovery Key Share Holders' Storage Master Key Cards were generated in 2010, and should be tested for functionality, then replaced due to age. This will be achieved by performing the following steps:

- Generate a new temporary SMK on the HSM
- Attempt to import an APP key backup encrypted with the production SMK (with an expected failed result). This will demonstrate incompatibility between the temporary SMK and the APP key backup
- Import the production SMK to the HSM using the 2010-era RKSH SMK Cards and successfully import the APP key backup. This will demonstrate compatibility between the production SMK and APP key Backup as well as functionality of the 2010-era RKSH SMK cards
- Generate replacement RKSH SMK cards to replace the existing cards due to age
- Destroy the 2010-era RKSH SMK cards

Note: For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.

HSM5E (Tier 7) Setup

Step	Activity	Initials	Time
5.1	CA performs the following steps to prepare the HSM: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and the serial number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. **HSM5E: TEB # BB51184250 / Serial # H1903018** Last Verified: KSK Ceremony 51 2023-11-30 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	*(initials)*	19:17

Power ON HSM5E (Tier 7)

Step	Activity	Initials	Time
5.2	CA selects the **HSM Output** terminal window.	*(initials)*	19:17
5.3	CA performs the following steps to prepare the HSM: a) Verify the label on the HSM reads **HSM5E**. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. Note: Status information should appear in the HSM output terminal window. d) Scroll up on the terminal window while IW verifies the displayed HSM serial number on the screen reads **H1903018**. e) Scroll down to the end of the terminal window. **HSM5E: Serial # H1903018** Note: The date and time on the HSM is not used as a reference for logging and timestamp.	*(initials)*	19:19

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 5 Step(s): 5.4 Page(s): 24 Date and time of the exception: 2024-04-25 19:35 Note: IW describes the exception(s) and action(s) below.		

The scripts for ceremonies 1 and 45 were not present. Aaron ~~print~~ looked up ceremony 1 on his phone from the IANA website and all TEBs from ceremony 1 were verified using that information. Andres looked up ceremony 45 on a phone from the IANA website and the single TEB from ceremony 45 was verified using that information.

Ceremony 31 was also not printed and Aaron used his phone to find that information which was used for verification.

Recovery Key Share Holders' (RKSHs) Credentials Verification

Step	Activity	Initials	Time
5.4	The CA calls each of the RKSHs listed below sequentially to perform the following steps: a) RKSH reads aloud the TEB number, then CA inspects it for tamper evidence while the IW verifies its "last verified" information using the specified previous ceremony script. b) RKSH and CA open the TEB, then the CA removes the contents to perform the action specified below. **RKSH2: Ondřej Surý** **TEB # A14377098** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH3: Kristian Ørmen** **TEB # BB46592121** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 31 2017-10-18 **RKSH4: Jiankang Yao** **TEB # A14377104** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH5: Bevil Wooding** **TEB # A14377106** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH6: John Curran** **TEB # A14377108** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 1 2010-06-16 **RKSH7: Dave Lawrence** **TEB # BB91951260** (RKSH places cards on their designated card holder) Last Verified: KSK Ceremony 45 2022-05-12 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	*[initials]*	A:41

APP Key Backups

Step	Activity	Initials	Time
5.5	CA performs the following steps to prepare the APP key backups: a) Remove the TEB from the cart and place it on the ceremony table. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Open and discard the TEB, and if not already present, place a corresponding label on the APP key Backup plastic case. e) Remove the APP key cards and place them on the card holder, ensuring their respective backup HSMFDs remain in their plastic case. f) Place the plastic case along with its corresponding sheet of paper with the printed HSMFD hash on its designated area of the ceremony table. **KSK-2023: TEB # BB02638661** Last Verified: KSK Ceremony 51 2023-11-30 Note: "Last verified" indicates the most recent time materials were placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	*[initials]*	19:43

Delete the Specified KSK from the HSM

Step	Activity	Initials	Time
5.6	CA performs the following steps to list the KSK(s) present in the HSM: 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 a randomly selected CO card. d) When **"PIN?"** is displayed, enter **"11223344"**, then press **ENT**. e) When **"Remove Card?"** is displayed, remove the CO card. f) Repeat steps **c)** to **e)** for the 2nd and 3rd CO cards. g) Select **"2.Key Details"**, press **ENT** to confirm. h) When **"List Keys?"** is displayed, press **ENT**. i) Select **"1.Key Summary"**, press **ENT** to confirm. j) When **"Key Summary?"** is displayed, press **ENT**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 2 1st CO card _Z_ of 7 2nd CO card _7_ of 7 3rd CO card _4_ of 7 Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.	_M_	19:45
5.7	CA matches the displayed KSK label(s) in the **HSM Output** terminal window. **KSK-2017: Klajeyz** **KSK-2023: Kmrfl3b**	_M_	19:46
5.8	CA performs the following steps to delete the specified KSK(s) from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"7.Erase App Keys"**, press **ENT** to confirm. d) When "Erase App Keys?" is displayed, press **ENT** to confirm. e) Select **"2.Specify Key"**, press **ENT** to confirm. f) Select the **Kmrfl3b** key by pressing > to move it to the top of the HSM's display, then press **"A"** to select **Kmrfl3b**, then press < to see the key list. **Verify the (*) asterisk is next to Kmrfl3b** then press **ENT** to confirm. **There is no system confirmation prompt.** g) When **Done** is displayed, press **ENT** to return to the App Keys Menu. h) Press **CLR** to return to the Key Mgmt menu.	_M_	19:48
5.9	CA performs the following steps to list the KSK from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. CA confirms that the **KSK-2023: Kmrfl3b** has been deleted	_M_	19:48

Generate a Temporary SMK

Step	Activity	Initials	Time
5.10	CA performs the following steps to generate a temporary SMK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"1.Generate SMK"**, press **ENT** to confirm. d) When **"Generate SMK?"** is displayed, press **ENT** to confirm. e) When **"SMK Generated"** is displayed, press **ENT** to confirm. f) Press **CLR** once to return to the menu **"Key Mgmt"**.	_(initials)_	19:49

Attempt to Import the APP Key Backup (Anticipating a Failed Result)

Step	Activity	Initials	Time
5.11	CA performs the following steps to attempt to import the specified key to demonstrate incompatibility between the temporary SMK and the APP key backup: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required APP key card. g) When **"Remove Card?"** is displayed, remove the APP key card. h) When **"SMK Mismatch"** is displayed, press **ENT** to confirm. i) When **"Restore failed Error code 120D"** is displayed, press **ENT** to confirm. j) Press **CLR** once to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. **KSK-2023: Kmrfl3b** APP Key card # 2 Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.	_(initials)_	19:51
5.12	CA performs the following steps to list the KSK from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**. CA confirms that the **KSK-2023: Kmrfl3b** is still not present in the HSM	_(initials)_	19:52

Import the Production SMK Using 2010-era RKSH SMK Cards

Step	Activity	Initials	Time
5.13	CA performs the following steps to import the production SMK: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"3.Restore SMK"**, press **ENT** to confirm. d) When **"Restore SMK?"** is displayed, press **ENT** to confirm. e) When **"Insert Card SMK #X?"** is displayed, insert a randomly selected RKSH SMK card. f) When **"Remove Card?"** is displayed, remove the RKSH SMK card. g) Repeat steps **e)** to **f)** for the 2nd, 3rd, 4th, and 5th RKSH SMK cards. h) When **"SMK Restored"** is displayed, press **ENT** to confirm. i) Press **CLR** once to return to the menu **"Key Mgmt"**. IW records which cards were used below. Each card is returned to its designated card holder after use. Set # 1 1st RKSH SMK card __5__ of 7 2nd RKSH SMK card __6__ of 7 3rd RKSH SMK card __2__ of 7 4th RKSH SMK card __7__ of 7 5th RKSH SMK card __3__ of 7 Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.	_M_	19:56

Import the APP key Backup (Anticipating a Successful Result)

Step	Activity	Initials	Time
5.14	CA performs the following steps to import the specified key to demonstrate compatibility between the production SMK and the APP key backup: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"3.App Keys"** from the current **"Key Mgmt"** menu, press **ENT** to confirm. c) Select **"2.Restore"**, press **ENT** to confirm. d) When **"Restore?"** is displayed, press **ENT** to confirm. e) When **"Which Media?"** is displayed, select **"2. From Card"**, press **ENT** to confirm. f) When **"Insert Card #X?"** is displayed, insert the required APP key card. g) When **"Remove Card?"** is displayed, remove the APP key card. h) When **"Restore Complete"** is displayed, press **ENT** to confirm. i) Press **CLR** once to return to the menu **"Key Mgmt"**. CA uses the card listed below. Card is returned to its designated card holder after use. **KSK-2023: Kmrfl3b** APP Key card # 2 Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of credential roles and their purpose see Appendix A number [14] and [15] on page 41.	_M_	19:57

List the KSKs present in the HSM

Step	Activity	Initials	Time
5.15	CA performs the following steps to list the KSK from the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Key Details"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) When **"List Keys?"** is displayed, press **ENT**. d) Select **"1.Key Summary"**, press **ENT** to confirm. e) When **"Key Summary?"** is displayed, press **ENT**.	*M*	20:00
5.16	CA matches the displayed KSK label(s) in the **HSM Output** terminal window. **KSK-2017: Klajeyz** **KSK-2023: Kmrfl3b**	*M*	20:00

Remove the 2010-era RKSH SMK Cards from the Card Holder for Pending Destruction

Step	Activity	Initials	Time
5.17	CA performs the following steps to prepare the 2010-era RKSH SMK cards for destruction: a) Gather set 1 of the 2010-era RKSH SMK cards and place them in an available empty plastic case. b) Set the plastic case aside on the ceremony table for pending destruction. c) Gather set 2 of the 2010-era RKSH SMK cards and place them in an available empty plastic case. d) Set the plastic case aside on the ceremony table for pending destruction.	*M*	20:02

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 5 Step(s): 5,19 Page(s): 29 Date and time of the exception: 2024-04-25 20:30 Note: IW describes the exception(s) and action(s) below.	$\mathcal{M}$	20:30

Step f says to use "7" when entering the number of cards, but only six cards were present and we entered "6".
Card 3 of 7 of Set 2 did not read properly. CA wiped the contacts, and the process was repeated from card 3 with cards 4, 5, 6, and 7.

Generate Two New Sets of RKSH SMK Cards

Step	Activity	Initials	Time
5.18	CA performs the following steps to issue Recovery Key Share Holder (RKSH) Storage Master Key (SMK) cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"2.Backup SMK"**, press **ENT** to confirm. d) When **"Backup SMK?"** is displayed, press **ENT** to confirm. e) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**. f) When **"Num Req Cards?"** is displayed, enter **"5"**, then press **ENT**. g) When **"Insert Card #X?"** is displayed, insert the required RKSH SMK card. h) When **"Remove Card?"** is displayed, remove the RKSH SMK card. i) Repeat steps **g)** to **h)** until all the SMK cards have been issued. j) When **"Verify Card #X?"** is displayed, insert the required RKSH SMK card. k) When **"Remove Card?"** is displayed, remove the RKSH SMK card. l) Repeat steps **j)** to **k)** until all the RKSH SMK cards have been verified. m) When **"SMK Backed Up"** is displayed, press **ENT** to confirm. n) Repeat steps **c)** to **m)** to create a 2nd SMK card set. o) Press **CLR** once to return to the menu **"Key Mgmt"**.	_(initials)_	20:18

Clear and Destroy 2010-era RKSH SMK Cards

Step	Activity	Initials	Time
5.19	CA performs the following steps to clear the 2010-era RKSH SMK Cards: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"4.SMK"** from the same menu **"Key Mgmt"**, press **ENT** to confirm. c) Select **"4.Clear Cards"**, press **ENT** to confirm. d) When **"Clear Cards?"** is displayed, press **ENT** to confirm. e) When **"Insert Card SMK #X?"** is displayed, take the **SMK #X** card, show the **SMK #X** card to the audit camera and then insert the **SMK #X** card into the HSM's card reader. f) When **"Num Cards?"** is displayed, enter **"7"**, then press **ENT**. g) When **"Clearing Card Are you sure?"** is displayed, press **ENT** to confirm. h) When **"Remove Card?"** is displayed, remove the SMK card. i) Repeat steps **e)** to **h)** skipping **f)** for the remaining cards in this SMK set. j) Repeat steps **c)** to **i)** for the 2nd SMK set. k) Press **CLR twice** to return to the main menu **"Secured"**.	_(initials)_	20:30
5.20	CA uses the shredder to destroy the cleared 2010-era RKSH SMK Cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.	_(initials)_	20:31

Handwritten note (right margin, near step 5.19): Card 3 of 7 malfunctioned

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 5 Step(s): 5.21 Page(s): 30 Date and time of the exception: 2024-04-25 2018 Note: IW describes the exception(s) and action(s) below.	_M_	20:38

The step required us to disconnect ethernet but ethernet was never plugged in.

Place HSM5E (Tier 7) into a TEB

Step	Activity	Initials	Time
5.21	CA switches the HSM power **OFF**, then disconnects the power, serial, and ethernet connections. Note: DO NOT unplug the cable connections on the laptop.	*M*	20:38
5.22	CA performs the following steps to prepare the HSM for storage: a) Ask the IW for the HSM's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. **HSM5E: TEB # BB51184554 / Serial # H1903018**	*M*	20:41

Return the APP key backup into a TEB

Step	Activity	Initials	Time
5.23	CA performs the following steps to prepare the APP key backup for storage: a) Ask the IW for the APP key backup's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Place the APP key backup into its plastic case along with the backup HSMFD c) Place the the plastic case and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the APP key backup TEB onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the APP key backup TEB on the cart. **KSK-2023: TEB # BB02639665**	*M*	20:45

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: 5 Step(s): 5.24 Page(s): 32 Date and time of the exception: 2024-04-25 21:20 Note: IW describes the exception(s) and action(s) below.	*(signature)*	21:20
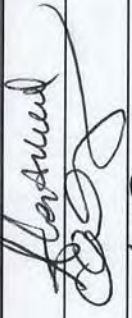
The set of bags for RKSH1 were incorrectly marked, ~~and~~ and recorded in the script. We modified the script to have the new bag numbers.

For RKSH4 the primary bag was accidently placed in the backup bag. The backup bag had to be destroyed and replaced. The new TEB was recorded in the script.

An extra TEB strip was collected due to this error.

Place Recovery Key Share Holders' Credentials into TEBs

Step	Activity	Initials	Time
5.24	The CA calls each of the RKSHs listed below sequentially to the ceremony table to perform the following steps: a) CA asks the IW for the RKSH's designated new primary TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. b) CA asks the IW for the RKSH's designated new backup TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. c) CA places the backup TEB inside of the primary TEB in case the primary TEB is compromised in the future. d) CA places the RKSH note inside of the primary TEB, ensuring it's still legible through the bag. e) RKSH removes their credentials from the card holder, then hands them to the CA. f) CA verifies the credentials, then places them into an available plastic case. g) CA places the plastic case into its designated new TEB, then seals it. h) CA gives the IW sealing strips for post-ceremony inventory. i) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. j) CA initials the TEB with a ballpoint pen. k) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. l) CA gives the TEB containing the cards to the RKSH. m) RKSH inspects the TEB, verifies its contents, then initials it with a ballpoint pen. n) RKSH writes the date and time, signs the credential table of the IW's script, then the IW initials the entry. o) RKSH returns to their seat with their TEB. p) Repeat steps for all the remaining RKSHs' credentials on the list. **RKSH1: Sebastian Castro** **Keyper Credential Primary TEB #** BB02639664 *BB02638649* **Keyper Credential Backup TEB #** BB02639663 *BB02639648* **RKSH2: Ondřej Surý** **Keyper Credential Primary TEB #** BB02639662 **Keyper Credential Backup TEB #** BB02639661 **RKSH3: Kristian Ørmen** **Keyper Credential Primary TEB #** BB02639660 **Keyper Credential Backup TEB #** BB02639659 **RKSH4: Jiankang Yao** **Keyper Credential Primary TEB #** BB02639658 **Keyper Credential Backup TEB #** BB02639657 *Destroyed BB9195iz41* **RKSH5: Bevil Wooding** **Keyper Credential Primary TEB #** BB02639656 **Keyper Credential Backup TEB #** BB02639655 **RKSH6: John Curran** **Keyper Credential Primary TEB #** BB02639654 **Keyper Credential Backup TEB #** BB02639653 **RKSH7: Dave Lawrence** **Keyper Credential Primary TEB #** BB02639652 **Keyper Credential Backup TEB #** BB02639651	_M_	21:39

Act 5: Test and Replace Recovery Key Share Holders' (RKSHs) Storage Master Key (SMK) Cards

TCR	TEB #	Printed Name	Signature	Date	Time	IW Initials
RKSH1	TEB # BB02639664 BB02639649	Sebastian Castro		2024 Apr 25	20:52	
RKSH2	TEB # BB02639662	Ondřej Surý		2024 Apr 25	20:57	
RKSH3	TEB # BB02639660	Kristian Ørmen		2024 Apr 25	21:00	
RKSH4	TEB # BB02639658	Jiankang Yao		2024 Apr 25	21:10	
RKSH5	TEB # BB02639656	Bevil Wooding		2024 Apr 25	21:13	
RKSH6	TEB # BB02639654	John Curran		2024 Apr 25	21:16	
RKSH7	TEB # BB02639652	Dave Lawrence		2024 Apr 25	21:18	

script-20240425.log

Script started on 2024-04-25 18:23:15+00:00 [TERM="xterm-256color" TTY="/dev/pts/1" COLUM
NS="72" LINES="23"]
\033[?2004h(kskm) root@coen:/media/HSMFD# ping hsm
NONG[MBR04[192.168.0.2) 56(84) bytes of data.
\033[?2004l18:36:15.667: kskm-ksrsigner
X023[?2004l18:36:15.667: kskm-ksrsigner
64 bytes from hsm (192.168.0.2): icmp_seq=1 ttl=255 time=0.901 ms
64 bytes from hsm (192.168.0.2): icmp_seq=2 ttl=255 time=0.608 ms
64 bytes from hsm (192.168.0.2): icmp_seq=3 ttl=255 time=0.744 ms
64 bytes from hsm (192.168.0.2): icmp_seq=4 ttl=255 time=0.616 ms
^C

--- hsm ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.608/0.717/0.901/0.119 ms
\033[?2004h(kskm) root@coen:/media/HSMFD# cd /media/KSRFD/KSR\00753-1
\033[?2004h(kskm) root@coen:/media/KSRFD/KSR53-1# kskm-ksrsigner
r.yaml SHA-256 962c015dd68bee5380fd50e2eec98dfe0c97if6634c2b21le9444a3b2ffe179f9 WORDS pre
fer Chicago drunken filament stockman Medusa tycoon enterprise merit Wyoming drumbeat tom
orrow tumor narrative talon tobacco spearhead hideaway village Galveston drainage council
man blackjack Burlington Pluto designing reform pioneer Zulu tolerance jawbone Waterloo
2024-04-25 18:36:15,706: kskm.common.config: INFO Configuration validated
2024-04-25 18:36:15,708: kskm.skr.load: INFO Loaded SKR from file skr-root-2024-q2-0.xml
SHA-256 d6b445c09306a9cb44d99cb77321085b53b1fd6b6d73d488f95857lf631dd62 WORDS stockman p
oliteness crusade recipe playhouse amulet revenge revival crumpled supportive python proc
essor hockey Camelot aimless exodus dwelling photograph willow gravity Scotland stethosco
pe commence dictator payday Montana music hideaway village company swelter gadgetry
2024-04-25 18:36:15,948: kskm.tools.ksrsigner: INFO Previous SKR:
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO # Inception   Expiration

        ZSK Tags   KSK(CKA_LABEL)
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 1   2024-04-01T00:00:00 2024-04-22T00:
00:00 30903,5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 2   2024-04-11T00:00:00 2024-05-02T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 3   2024-04-21T00:00:00 2024-05-12T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 4   2024-05-01T00:00:00 2024-05-22T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 5   2024-05-11T00:00:00 2024-06-01T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 6   2024-05-21T00:00:00 2024-06-11T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 7   2024-05-31T00:00:00 2024-06-21T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 8   2024-06-10T00:00:00 2024-07-01T00:
00:00 5613   20326(Klajeyz)/S
2024-04-25 18:36:15,949: kskm.tools.ksrsigner: INFO 9   2024-06-20T00:00:00 2024-07-11T00:
00:00 20038,5613   20326(Klajeyz)/S
2024-04-25 18:36:15,950: kskm.ksr.load: INFO Loaded KSR from file ksr-root-2024-q3-0.xml
SHA-256 51ffea38b7a12d8a1290155c570e17a366408e1b5bff642463e13b09b8254f705 WORDS drunken Yu
catan Trojan consulting seabird outfielder bluebird Jupiter atlas millionaire edict resis
tor guidance tolerance keyboard congregate flytrap antenna tempest positive slingshot voc
alist crowfoot detergent concert barbecue ruffled narrative sawdust equation virus almigh
ty
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO Validating KSR using request policy:
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   dataclass_placeholder: None
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   acceptable_domains: ['.']
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   approved_algorithms: ['RSASHA256']
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_bundle_intervals: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_bundle_overlap: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_chain_keys: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_chain_keys_in_hsm: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_chain_overlap: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_cycle_length: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_keys_match_ksk_operator_policy:
True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_keys_publish_safety: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   check_keys_retire_safety: True
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   dns_ttl: 172800
2024-04-25 18:36:15,953: kskm.ksr.validate: INFO   enable_unsupported_ecdsa: False
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   keys_match_zsk_policy: True
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   max_bundle_interval: 11 days, 0:00:00
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   max_cycle_inception_length: 81 days, 0
:00:00
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   min_bundle_interval: 9 days, 0:00:00
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   min_cycle_inception_length: 79 days, 0
:00:00
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   num_bundles: 9
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   num_different_keys_in_all_bundles: 3
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   num_keys_per_bundle: [2, 1, 1, 1, 1, 1
, 1, 1, 2]
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   rsa_approved_exponents: [65537]
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   rsa_approved_key_sizes: [2048]
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   rsa_exponent_match_zsk_policy: True
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   signature_algorithms_match_zsk_policy:
True
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   signature_check_expire_horizon: True
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   signature_horizon_days: 180
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   signature_validity_match_zsk_policy: T
rue
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO   validate_signatures: True
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO KSR-DOMAIN: Verified domain '.'
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO KSR-ID: Will be checked later, when SKR
is available
2024-04-25 18:36:15,954: kskm.ksr.validate: INFO KSR-BUNDLE-UNIQUE: All 9 bundles have un
ique ids
2024-04-25 18:36:15,955: kskm.ksr.validate: INFO KSR-BUNDLE-KEYS: All 3 unique keys in th
e bundles accepted by policy
2024-04-25 18:36:15,956: kskm.ksr.validate: INFO KSR-BUNDLE-POP: All 9 bundles contain pr
oof-of-possession
2024-04-25 18:36:15,956: kskm.ksr.validate: INFO KSR-BUNDLE-COUNT: Number of bundles (9)
accepted
2024-04-25 18:36:15,956: kskm.ksr.validate: INFO KSR-BUNDLE-CYCLE-DURATION: The cycle len
gth is in accordance with the KSK operator policy
2024-04-25 18:36:15,956: kskm.ksr.validate: INFO KSR-POLICY-KEYS: Validated number of key
s per bundle, and for all bundles
2024-04-25 18:36:15,956: kskm.ksr.validate: INFO KSR-POLICY-ALG: All 1 ZSK operator signa
ture algorithms accepted by policy
2024-04-25 18:36:15,956: kskm.ksr.validate: INFO KSR-POLICY-SIG-OVERLAP: All bundles over
lap in accordance with the stated ZSK operator policy
2024-04-25 18:36:15,957: kskm.ksr.validate: INFO KSR-POLICY-SIG-VALIDITY: All signatures e
xpire in less than 180 days
2024-04-25 18:36:15,957: kskm.ksr.validate: INFO KSR-POLICY-SIG-HORIZON: All bundles
intervals in accordance with the KSK operator policy
2024-04-25 18:36:15,957: kskm.ksr.validate: INFO   ave 21 days <= validity >= 21 days
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO Request:
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO # Inception   Expiration

        ZSK Tags   KSK(CKA_LABEL)
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 1   2024-07-01T00:00:00 2024-07-22T00:
00:00 20038,5613
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 2   2024-07-11T00:00:00 2024-08-01T00:
00:00 20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 3   2024-07-21T00:00:00 2024-08-11T00:
00:00 20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 4   2024-07-31T00:00:00 2024-08-21T00:
00:00 20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 5   2024-08-10T00:00:00 2024-08-31T00:
00:00 20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 6   2024-08-20T00:00:00 2024-09-10T00:

```
00:00  20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 7  2024-08-30T00:00:00 2024-09-20T00:
00:00  20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 8  2024-09-09T00:00:00 2024-09-30T00:
00:00  20038
2024-04-25 18:36:15,957: kskm.tools.ksrsigner: INFO 9  2024-09-19T00:00:00 2024-10-10T00:
00:00  20038,61050
2024-04-25 18:36:15,957: kskm.misc.hsm: INFO Initializing PKCS#11 module aep using /opt/K
eyper/PKCS11Provider/pkcs11.linux.gcc_4_1_2_glibc_2.5_x86_64.so.5.02
2024-04-25 18:36:16,214: kskm.misc.hsm: INFO HSM First slot:      ICANNKSK

2024-04-25 18:36:16,214: kskm.misc.hsm: INFO HSM Manufacturer ID: Ultra Electronics AEP N
etworks
2024-04-25 18:36:16,214: kskm.misc.hsm: INFO HSM Model:        Keyper 9860-2
2024-04-25 18:36:16,214: kskm.misc.hsm: INFO HSM Serial:       H2110009
2024-04-25 18:36:16,214: kskm.signer.verify_chain: INFO Checking coherence between SKR(n-
1) and this KSR
2024-04-25 18:36:16,215: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: The last keys in
SKR(n-1) matches the first keys in this KSR
2024-04-25 18:36:16,215: kskm.signer.verify_chain: INFO KSR-CHAIN-OVERLAP: Overlap with 1
ast bundle in SKR(n-1) 10 days is in accordance with the KSR policy
2024-04-25 18:36:16,216: kskm.signer.verify_chain: INFO KSR-CHAIN-KEYS: All 1 signatures
in the last bundle of the last SKR were made with keys present in the HSM(s)

FILENAME:    ksr-root-2024-q3-0.xml
SHA-256 HEX:    51ffea38b7a12484129055c570e17a36640e1b5bff642463e13b098b254f705
SHA-256 WORDS:  drunken Yucatan Trojan consulting seabird outfielder bluebird Jupiter atl
est positive slingshot vocalist crowfoot detergent concert barbecue ruffled narrative saw
dust equation virus almighty

Sign KSR? Confirm with "yes" (exactly) or anything else to abort: Yes
2024-04-25 18:39:32,026: kskm.signer.policy: INFO KSR-POLICY-SAFETY: Publishsafety valida
ted
2024-04-25 18:39:32,026: kskm.signer.policy: INFO KSR-POLICY-SAFETY: Retiresafety validat
ed
2024-04-25 18:39:32,026: kskm.tools.ksrsigner: INFO Generated SKR:
2024-04-25 18:39:32,026: kskm.tools.ksrsigner: INFO # Inception           Expiration
2KSK Tags   KSK (CKA_LABEL)
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 1  2024-07-01T00:00:00 2024-07-22T00:
00:00  20038,5613    20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 2  2024-07-11T00:00:00 2024-08-01T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 3  2024-07-21T00:00:00 2024-08-11T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 4  2024-07-31T00:00:00 2024-08-21T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 5  2024-08-10T00:00:00 2024-08-31T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 6  2024-08-20T00:00:00 2024-09-10T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 7  2024-08-30T00:00:00 2024-09-20T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 8  2024-09-09T00:00:00 2024-09-30T00:
00:00  20038         20326(Klajeyz)/S
2024-04-25 18:39:32,027: kskm.tools.ksrsigner: INFO 9  2024-09-19T00:00:00 2024-10-10T00:
00:00  20038,61050   20326(Klajeyz)/S
2024-04-25 18:39:32,155: kskm.signer: INFO Wrote SKR to file skr-root-2024-q3-0.xml SHA-2
56 bb9a51634bf36822e0e4c7e7b0f69725b9f6484a6dd367B0a1f5e482a992279 WORDS shamrock newsle
tter drunken Galveston crucial hemisphere erase opulent flytrap Jupiter rematch tambourine
ent kickoff atmosphere gazelle holiness eyeglass dictator brickyard nebula blockade inertia
Christmas indigo allow businessman drainage insurg
103E19203A257(kbg)18oot@coen:/media/KSRFD/KSK53-1# printlog kskm-ksrsigner-20240425-1
\0236$080#41 1 copy | sent to printer
```

```
6 lines were wrapped
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK53-1# cd /media/HSMFD/
\033[?2004l(kskm) root@coen:/media/HSMFD# ls -ltrR /media/KSRFD/
X033[?2004h@SMFD/:
total 32
drwxr-xr-x 2 root root 16384 Apr 16 18:27 \033[0m\033[01;34mKSK53-2\033[0m
drwxr-xr-x 2 root root 16384 Apr 25 18:39 \033[01;34mKSK53-1\033[0m

/media/KSRFD/KSK53-2:
-rw-r--r-- 1 root root 11188 Apr 16 18:27 ksrsigner.yaml

/media/KSRFD/KSK53-1:
total 128
-rw-r--r-- 1 root root 24824 Apr 16 18:27 skr-root-2024-q2-0.xml
-rw-r--r-- 1 root root 11501 Apr 16 18:27 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Apr 16 18:27 ksr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 24832 Apr 25 18:39 skr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 11078 Apr 25 18:39 skm-ksrsigner-20240425-18361S-13267.log
\033[?2004h(kskm) root@coen:/media/HSMFD# cp -pR /media/KSRFD/*
\033[?2004h(kskm) root@coen:/media/HSMFD# cp -pR /media/KSRFD/*.
\033[?2004l(kskm) root@coen:/media/HSMFD# ls -ltrR
\033[?22004l
total 3472
-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 Kjgmt7v.csr
-rw-r--r-- 1 root root 36864 Jun 16 2010 ttyaudit-ttyUSB1-20100616-182157.log
-rw-r--r-- 1 root root 45056 Jun 16 2010 ttyaudit-ttyUSB0-20100616-182157.log
-rw-r--r-- 1 root root 18364 Jun 16 2010 skr-root-2010-q3-2.xml
-rw-r--r-- 1 root root  4473 Jun 16 2010 ksrsigner-20100616-214329.log
-rw-r--r-- 1 root root 196608 Jun 16 2010 script-20100616.log
-rw-r--r-- 1 root root  7674 Jun 16 2010 script-20100616-2209utc.log
-rw-r--r-- 1 root root 18364 Oct 31 2010 skr.xml.20101010181303
-rw-r--r-- 1 root root 15547 Oct 31 2010 ksr-root-2011-q1-0.xml
-rw-r--r-- 1 root root 18402 Nov  1 2010 skr-root-2011-q1-0.xml
-rw-r--r-- 1 root root  5504 Nov  1 2010 ksrsigner-20101101-181303.log
-rw-r--r-- 1 root root 14005 Nov  1 2010 ttyaudit-ttyUSB0-20101101-175457.log
-rw-r--r-- 1 root root  7161 Nov  1 2010 script-20101101.log
-rw-r--r-- 1 root root 18402 Feb  7 2011 skr.xml.20110511181632
-rw-r--r-- 1 root root 15547 Apr 25 2011 ksr-root-2011-q3-0.xml
-rw-r--r-- 1 root root  1400 May 11 2011 ksrsigner-20110511-191351.log
-rw-r--r-- 1 root root 18402 May 11 2011 skr-root-2011-q3-0.xml
-rw-r--r-- 1 root root  5510 May 11 2011 ksrsigner-20110511-181632.log
-rw-r--r-- 1 root root 14374 May 11 2011 ttyaudit-ttyUSB0-20110511-180559.log
-rw-r--r-- 1 root root  9133 May 11 2011 script-20110511.log
-rw-r--r-- 1 root root 18404 Jul 20 2011 skr.xml.20110930181607
-rw-r--r-- 1 root root 15587 Sep 23 2011 ksr-root-2012-q1-0.xml
-rw-r--r-- 1 root root 18422 Sep 30 2011 skr-root-2012-q1-0.xml
-rw-r--r-- 1 root root  5609 Sep 30 2011 ksrsigner-20110930-181607.log
-rw-r--r-- 1 root root 12034 Sep 30 2011 ttyaudit-ttyUSB0-20110930-180703.log
-rw-r--r-- 1 root root  7270 Sep 30 2011 script-20110930.log
-rw-r--r-- 1 root root 18424 Feb  2 2012 skr.xml.20120522151741
-rw-r--r-- 1 root root 15571 May  9 2012 ksr-root-2012-q3-0.xml
-rw-r--r-- 1 root root 18814 May 22 2012 skr-root-2012-q3-0.xml
-rw-r--r-- 1 root root  5528 May 22 2012 ksrsigner-20120522-151741.log
-rw-r--r-- 1 root root 12034 May 22 2012 ttyaudit-ttyUSB0-20120522-150621.log
-rw-r--r-- 1 root root 13817 May 22 2012 script-20120522.log
-rw-r--r-- 1 root root 18324 Jul 26 2012 skr.xml.20121112155152
-rw-r--r-- 1 root root 15371 Oct 12 2012 ksr-root-2013-q1-0.xml
-rw-r--r-- 1 root root 18314 Nov 12 2012 skr-root-2013-q1-0.xml
-rw-r--r-- 1 root root  5529 Nov 12 2012 ksrsigner-20121112-155152.log
```

```
-rw-r--r-- 1 root root 12044 Nov 12 2012 ttyaudit-ttyUSB0-20121112-154229.log
-rw-r--r-- 1 root root 12249 Nov 12 2012 script-20121112.log
-rw-r--r-- 1 root root 18314 Feb 12 2013 skr.xml.20130502190633
-rw-r--r-- 1 root root 15371 Apr  5 2013 ksr-root-2013-q3-0.xml
-rw-r--r-- 1 root root  4004 May  2 2013 ksrsigner-20130502-190252.log
-rw-r--r-- 1 root root 18314 May  2 2013 skr-root-2013-q3-0.xml
-rw-r--r-- 1 root root  5502 May  2 2013 ksrsigner-20130502-190633.log
-rw-r--r-- 1 root root 12397 May  2 2013 ttyaudit-ttyUSB0-20130502-185222.log
-rw-r--r-- 1 root root 21494 May  2 2013 script-20130502.log
-rw-r--r-- 1 root root 18314 Aug  7 2013 skr.xml.20131024184618
-rw-r--r-- 1 root root 15371 Oct  4 2013 ksr-root-2014-q1-0.xml
-rw-r--r-- 1 root root 18314 Oct 24 2013 skr-root-2014-q1-0.xml
-rw-r--r-- 1 root root  5512 Oct 24 2013 ksrsigner-20131024-184618.log
-rw-r--r-- 1 root root 12044 Oct 24 2013 ttyaudit-ttyUSB0-20131024-182843.log
-rw-r--r-- 1 root root  9167 Oct 24 2013 script-20131024.log
-rw-r--r-- 1 root root 18314 Feb 13 2014 skr.xml.20140417183604
-rw-r--r-- 1 root root 15353 Apr  3 2014 ksr-root-2014-q3-0.xml
-rw-r--r-- 1 root root 18314 Apr 17 2014 skr-root-2014-q3-0.xml
-rw-r--r-- 1 root root  5511 Apr 17 2014 ksrsigner-20140417-183604.log
-rw-r--r-- 1 root root 12034 Apr 17 2014 ttyaudit-ttyUSB0-20140417-182117.log
-rw-r--r-- 1 root root  5853 Apr 17 2014 script-20140417.log
-rw-r--r-- 1 root root 18314 Nov 10 2014 skr.xml.20141120201132
-rw-r--r-- 1 root root 15371 Nov 20 2014 ksr-root-2015-q1-0.xml
-rw-r--r-- 1 root root 18314 Nov 20 2014 skr-root-2015-q1-0.xml
-rw-r--r-- 1 root root  5490 Nov 20 2014 ksrsigner-20141120-201132.log
-rw-r--r-- 1 root root 12042 Nov 20 2014 ttyaudit-ttyUSB0-20141120-200407.log
-rw-r--r-- 1 root root  5462 Nov 20 2014 script-20141120-1.log
-rw-r--r-- 1 root root 15353 Apr  1 2015 ksr-root-2015-q3-0.xml
-rw-r--r-- 1 root root 18314 Apr  1 2015 skr.xml.20150409183038
-rw-r--r-- 1 root root  5511 Apr  9 2015 skr-root-2015-q3-0.xml
-rw-r--r-- 1 root root  5621 Apr  9 2015 ksrsigner-20150409-183038.log
-rw-r--r-- 1 root root 15774 Apr  9 2015 ttyaudit-ttyUSB0-20150409-180743.log
-rw-r--r-- 1 root root  5636 Apr  9 2015 ksrsigner-20150409-193635.log
-rw-r--r-- 1 root root 33966 Apr  9 2015 ttyaudit-ttyUSB0-20150409-190117.log
-rw-r--r-- 1 root root  5636 Apr  9 2015 ksrsigner-20150409-205227.log
-rw-r--r-- 1 root root 34895 Apr  9 2015 ttyaudit-ttyUSB0-20150409-202837.log
-rw-r--r-- 1 root root 19175 Apr  9 2015 script-20150409.log
-rw-r--r-- 1 root root 18314 Nov  4 2015 skr.xml.20151112193232
-rw-r--r-- 1 root root 15371 Nov  4 2015 ksr-root-2016-q1-0.xml
-rw-r--r-- 1 root root  5547 Nov 12 2015 skr-root-2016-q1-0.xml
-rw-r--r-- 1 root root 12215 Nov 12 2015 ttyaudit-ttyUSB0-20151112-191111.log
-rw-r--r-- 1 root root  7282 Nov 12 2015 script-20151112.log
-rw-r--r-- 1 root root 18314 Apr 29 2016 skr.xml.20160512192325
-rw-r--r-- 1 root root 14301 Apr 29 2016 ksr-root-2016-q3-fallback-1.xml
-rw-r--r-- 1 root root 18314 Apr 29 2016 skr.xml.20160512190619
-rw-r--r-- 1 root root 15994 Apr 29 2016 ksr-root-2016-q3-0.xml
-rw-r--r-- 1 root root 18599 May 12 2016 skr-root-2016-q3-0.xml
-rw-r--r-- 1 root root  5534 May 12 2016 ksrsigner-20160512-190619.log
-rw-r--r-- 1 root root 17908 May 12 2016 skr-root-2016-q3-fallback-1.xml
-rw-r--r-- 1 root root  5566 May 12 2016 ksrsigner-20160512-192325.log
-rw-r--r-- 1 root root 12484 May 12 2016 ttyaudit-ttyUSB0-20160512-184752.log
-rw-r--r-- 1 root root 15870 May 12 2016 script-20160512.log
-rw-r--r-- 1 root root 19557 Oct 24 2016 ksr-root-2017-q1-0.xml
-rw-r--r-- 1 root root 21083 Oct 27 2016 skr.xml.20161027183803
-rw-r--r-- 1 root root 20348 Oct 27 2016 skr.xml
-rw-r--r-- 1 root root 20348 Oct 27 2016 skr-root-2017-q1-0.xml
-rw-r--r-- 1 root root  5501 Oct 27 2016 ksrsigner-20161027-183803.log
-rw-r--r-- 1 root root  2712 Oct 27 2016 ksrgen-20161027-184920.log
-rw-r--r-- 1 root root   817 Oct 27 2016 Klajeyz.csr
-rw-r--r-- 1 root root   357 Oct 27 2016 keybackup-20161027-185705.log
-rw-r--r-- 1 root root   357 Oct 27 2016 keybackup-20161027-200501.log
-rw-r--r-- 1 root root 28791 Oct 27 2016 ttyaudit-ttyUSB0-20161027-182428.log
-rw-r--r-- 1 root root 33568 Oct 27 2016 ttyaudit-ttyUSB0-20161027-202240.log

-rw-r--r-- 1 root root 17803 Oct 27 2016 script-20161027.log
-rw-r--r-- 1 root root  6505 Apr 27 2017 ksrsigner-20170427-183853.log
drwxr-xr-x 2 root root  8192 Apr 27 2017 \033[0m\033[01;34mKSK29-0-C_to_D\033[0m
-rw-r--r-- 1 root root  6228 Apr 27 2017 ksrsigner-20170427-184519.log
-rw-r--r-- 1 root root  8192 Apr 27 2017 \033[01;34mKSK29-1-D_to_C\033[0m
-rw-r--r-- 1 root root  6224 Apr 27 2017 ksrsigner-20170427-184912.log
drwxr-xr-x 2 root root  8192 Apr 27 2017 \033[01;34mKSK29-2-C_to_C\033[0m
-rw-r--r-- 1 root root 12913 Apr 27 2017 ttyaudit-ttyUSB0-20170427-182024.log
-rw-r--r-- 1 root root 16683 Apr 27 2017 script-20170427.log
-rw-r--r-- 1 root root     0 Oct 18 2017 script-20171018.log
-rw-r--r-- 1 root root  8192 Oct 18 2017 ttyaudit-ttyUSB0-20171018-174745.log
-rw-r--r-- 1 root root  6681 Oct 18 2017 ksrsigner-20171018-191941.log
-rw-r--r-- 1 root root  8192 Oct 18 2017 \033[01;34mKSK31-0-D_to_E\033[0m
drwxr-xr-x 2 root root  6698 Oct 18 2017 ksrsigner-20171018-182803.log
-rw-r--r-- 1 root root  8192 Oct 18 2017 \033[01;34mKSK31-1-E_to_D\033[0m
-rw-r--r-- 1 root root  6678 Oct 18 2017 ksrsigner-20171018-183150.log
drwxr-xr-x 2 root root  8192 Oct 18 2017 \033[01;34mKSK31-2-D_to_D\033[0m
-rw-r--r-- 1 root root  6361 Oct 18 2017 ksrsigner-20171018-183453.log
drwxr-xr-x 2 root root  8192 Oct 18 2017 \033[01;34mKSK31-3-C_to_C\033[0m
-rw-r--r-- 1 root root  4384 Oct 18 2017 ttyaudit-ttyUSB0-20171018-175253.log
-rw-r--r-- 1 root root 23163 Oct 18 2017 script-20171018-v2.log
-rw-r--r-- 1 root root 10002 Apr 11 2018 ttyaudit-ttyUSB0-20180411-181102.log
-rw-r--r-- 1 root root  6775 Apr 11 2018 ksrsigner-20180411-183203.log
drwxr-xr-x 2 root root  8192 Apr 11 2018 \033[01;34mKSK33-0-D_to_E\033[0m
-rw-r--r-- 1 root root  6783 Apr 11 2018 ksrsigner-20180411-183607.log
drwxr-xr-x 2 root root  8192 Apr 11 2018 \033[01;34mKSK33-1-E_to_D\033[0m
-rw-r--r-- 1 root root  6776 Apr 11 2018 ksrsigner-20180411-183814.log
drwxr-xr-x 2 root root  8192 Apr 11 2018 \033[01;34mKSK33-2-D_to_D\033[0m
-rw-r--r-- 1 root root  6469 Apr 11 2018 ksrsigner-20180411-184001.log
drwxr-xr-x 2 root root  8192 Apr 11 2018 \033[01;34mKSK33-3-C_to_C\033[0m
-rw-r--r-- 1 root root     0 Apr 11 2018 ttyaudit-ttyUSB0-20180411-185854.log
-rw-r--r-- 1 root root 36029 Apr 11 2018 script-20180411.log
-rw-r--r-- 1 root root  6757 Nov 15 2018 ttyaudit-ttyUSB0-20181115-194236.log
drwxr-xr-x 2 root root  8192 Nov 15 2018 \033[01;34mKSK35-0-E_to_F\033[0m
-rw-r--r-- 1 root root  6449 Nov 15 2018 ksrsigner-20181115-195208.log
drwxr-xr-x 2 root root  8192 Nov 15 2018 \033[01;34mKSK35-1-F_to_G\033[0m
-rwxr--r-- 1 root root  6775 Nov 15 2018 ksrsigner-20181115-195448.log
drwxr-xr-x 2 root root  8192 Nov 15 2018 \033[01;34mKSK35-2-E_to_E\033[0m
-rw-r--r-- 1 root root  6765 Nov 15 2018 ksrsigner-20181115-195652.log
drwxr-xr-x 2 root root  8192 Nov 15 2018 \033[01;34mKSK35-3-D_to_D\033[0m
-rw-r--r-- 1 root root 14444 Nov 15 2018 ttyaudit-ttyUSB0-20181115-192849.log
-rw-r--r-- 1 root root 39692 Nov 15 2018 script-20181115.log
drwxr-xr-x 2 root root  8192 May 16 2019 \033[01;34mKSK37\033[0m
-rw-r--r-- 1 root root  6271 May 16 2019 ksrsigner-20190516-190831.log
-rw-r--r-- 1 root root   357 May 16 2019 keybackup-20190516-200518.log
-rw-r--r-- 1 root root   210 May 16 2019 keybackup-20190516-200704.log
-rw-r--r-- 1 root root   271 May 16 2019 keybackup-20190516-200726.log
-rw-r--r-- 1 root root  6286 May 16 2019 keybackup-20190516-205655.log
-rw-r--r-- 1 root root 92098 May 16 2019 ttyaudit-ttyUSB0-20190516-185410.log
-rw-r--r-- 1 root root 30612 May 16 2019 script-20190516.log
-rw-r--r-- 1 root root  6263 Nov 14 2019 ttyaudit-ttyUSB0-20191114-190143.log
drwxr-xr-x 2 root root  8192 Nov 14 2019 \033[01;34mKSK39\033[0m
-rw-r--r-- 1 root root 52363 Nov 14 2019 ttyaudit-ttyUSB0-20191114-185111.log
-rw-r--r-- 1 root root 23869 Nov 14 2019 script-20191114.log
-rw-r--r-- 1 root root  6376 Oct 14 2021 ksrsigner-20211014-175632.log
drwxr-xr-x 2 root root  8192 Oct 14 2021 \033[01;34mKSK41\033[0m
-rw-r--r-- 1 root root  6391 Oct 14 2021 ksrsigner-20211014-190332.log
-rw-r--r-- 1 root root 64201 Oct 14 2021 ttyaudit-ttyUSB0-20211014-174505.log
-rw-r--r-- 1 root root 43058 Oct 14 2021 script-20211014.log
-rw-r--r-- 1 root root  6295 May 12 2022 ksrsigner-20220512-193033.log
drwxr-xr-x 2 root root  8192 May 12 2022 \033[01;34mKSK43\033[0m
-rw-r--r-- 1 root root 14456 May 12 2022 ttyaudit-ttyUSB0-20220512-191632.log
-rw-r--r-- 1 root root 25463 May 12 2022 script-20220512.log
-rw-r--r-- 1 root root  6265 Nov  3 2022 ksrsigner-20221103-181823.log
```

```
drwxr-xr-x 2 root root  8192 Nov  3  2022 \033[01;34mKSK47\033[0m
-rw-r--r-- 1 root root 15909 Nov  3  2022 ttyaudit-ttyS0-20221103-180106.log
drwxr-xr-x 2 root root 26616 Nov  3  2022 script-20221103.log
drwxr-xr-x 2 root root  8192 Apr 27  2023 \033[01;34mKSK49\033[0m
drwxr-xr-x 2 root root  6274 Apr 27  2023 \033[01;34mtmp\033[0m
-rw-r--r-- 1 root root  1072 Apr 27  2023 ksrsigner-20230427-181450.log
-rw-r--r-- 1 root root  1965 Apr 27  2023 kskm-keymaster-20230427-182232-931.log
-rw-r--r-- 1 root root  2961 Apr 27  2023 kskm-keymaster-20230427-182301-932.log
-rw-r--r-- 1 root root 46520 Apr 27  2023 KSKSlotDB.db
-rw-r--r-- 1 root root 51776 Apr 27  2023 script-20230427.log
drwxr-xr-x 4 root root  8192 Nov 30 19:24 \033[01;34mKSK51\033[0m
-rw-r--r-- 1 root root 94828 Nov 30 20:58 ttyaudit-ttyUSB0-20231130-190131.log
-rw-r--r-- 1 root root 65626 Nov 30 21:28 script-20231130.log
-rw-r--r-- 1 root root 13109 Apr 25 18:39 ttyaudit-ttyUSB0-20240425-182359.log
drwxr-xr-x 2 root root  8192 Apr 25 18:39 \033[01;34mKSK53-1\033[0m
drwxr-xr-x 3 root root  8192 Apr 25 18:42 \033[01;34mKSK53-2\033[0m

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

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

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

./KSK31-0-D_to_E:
total 128
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018181941
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q1-0-d_to_e.xml
-rw-r--r-- 1 root root  1344 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 24928 Oct 18  2017 skr-root-2018-q1-0-d_to_e.xml

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

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

./KSK31-3-C_to_C:
total 112
-rw-r--r-- 1 root root 24928 Oct 13  2017 skr.xml.20171018183453
-rw-r--r-- 1 root root 19556 Oct 13  2017 ksr-root-2018-q3-3-c_to_c.xml
-rw-r--r-- 1 root root  1148 Oct 13  2017 kskschedule.json
-rw-r--r-- 1 root root 20347 Oct 18  2017 skr.xml
-rw-r--r-- 1 root root 20347 Oct 18  2017 skr-root-2018-q3-3-c_to_c.xml

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

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

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

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

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

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

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

script-20240425.log

```
-rw-r--r-- 1 root root 24948 Nov 15 2018 skr.xml
-rw-r--r-- 1 root root 24948 Nov 15 2018 skr-root-2019-q1-2-e_to_e.xml

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

./KSK37:
total 104
-rw-r--r-- 1 root root 20369 Nov  8 2019 skr.xml.201905161901083:
-rw-r--r-- 1 root root 19600 May  8 2019 ksr-root-2019-q3-0.xml
-rw-r--r-- 1 root root  1148 May  8 2019 kskschedule.json
-rw-r--r-- 1 root root 20369 May 16 2019 skr.xml
-rw-r--r-- 1 root root 20369 May 16 2019 skr-root-2019-q3-0.xml

./KSK39:
total 104
-rw-r--r-- 1 root root 20369 Nov  6 2019 skr.xml.201911141901043
-rw-r--r-- 1 root root 19600 Nov  6 2019 ksr-root-2020-q1-0.xml
-rw-r--r-- 1 root root  1148 Nov  6 2019 kskschedule.json
-rw-r--r-- 1 root root 20369 Nov 14 2019 skr.xml
-rw-r--r-- 1 root root 20369 Nov 14 2019 skr-root-2020-q1-0.xml

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

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

./KSK47:
total 104
-rw-r--r-- 1 root root 20369 Jul 11 2018 skr.xml.20221103181823
-rw-r--r-- 1 root root 19564 Jul 11 2018 ksr-root-2023-q1-0.xml
-rw-r--r-- 1 root root  1148 Jul 11 2018 kskschedule.json
-rw-r--r-- 1 root root 20369 Nov  3 2022 skr.xml
-rw-r--r-- 1 root root 20369 Nov  3 2022 skr-root-2023-q1-0.xml

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

./tmp:
total 80
-rw-r--r-- 1 root root   880 May  2 2013 ksrsigner_20130502190252_5048_tmp_skr.xml
-rw-r--r-- 1 root root  1768 Apr 27 2023 skr.keybundle.8

-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.7
-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.6
-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.5
-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.4
-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.3
-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.2
-rw-r--r-- 1 root root  1392 Apr 27 2023 skr.keybundle.1
-rw-r--r-- 1 root root  1768 Apr 27 2023 skr.keybundle.0

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

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

./KSK51/HSM8E:
total 176
-rw-r--r-- 1 root root   652 Nov 17 22:23 style.xsl
-rw-r--r-- 1 root root 24833 Nov 17 22:23 skr-root-2023-q4-0.xml
-rw-r--r-- 1 root root 11507 Nov 17 22:23 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Nov 17 22:23 ksr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 11096 Nov 30 20:48 kskm-ksrsigner-20231130-204716-1058.log
-rw-r--r-- 1 root root 24832 Nov 30 20:48 HSM8E-skr-root-2024-q1-0.xml
-rw-r--r-- 1 root root 22205 Nov 30 20:51 current
-rw-r--r-- 1 root root 22205 Nov 30 20:51 new

./KSK53-1:
total 120
-rw-r--r-- 1 root root 24824 Apr 16 18:27 skr-root-2024-q2-0.xml
-rw-r--r-- 1 root root 11501 Apr 16 18:27 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Apr 16 18:27 ksr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 24832 Apr 25 18:39 skr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 11078 Apr 25 18:39 kskm-ksrsigner-20240425-183615-13267.log

./KSK53-2:
total 24
-rw-r--r-- 1 root root 11188 Apr 16 18:27 ksrsigner.yaml
drwxr-xr-x 2 root root  8192 Apr 25 18:39 \033[01;34mKSK53-1\033[0m

./KSK53-2/KSK53-1:
total 120
-rw-r--r-- 1 root root 24824 Apr 16 18:27 skr-root-2024-q2-0.xml
-rw-r--r-- 1 root root 11501 Apr 16 18:27 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Apr 16 18:27 ksr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 24832 Apr 25 18:39 skr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 11078 Apr 25 18:39 kskm-ksrsigner-20240425-183615-13267.log
\033[22004h(kskm) root@coen:/media/HSMFD# NOUY)0Qtis -ltrR /media/KSRFD/
\033[23004h(kskm) root@coen:/media/KSRFD/:
total 32
```

script-20240425.log

```
\033[?2004h(kskm) root@coen:/media/HSMFD# df -Bl /dev/sda
Filesystem       1B-blocks      Used Available Use% Mounted on
/dev/sda         602406912 602406912         0 100% /run/live/medium
\033[?2004h(kskm) root@coen:/media/HSMFD# head -c 602406912 /dev/sda | sha2wordlist
SHA256  2363d9c484e919b58bd45f413dedaed364712d72b3b7858c0fec5e3c52939dd8
PGP Words: blowtorch Galveston sugar reproduce mural ultimate bedlamp positive obtuse so
uvenir eyetooth decadence commence unify robust sociable flytrap hideaway button holiness
scallion processor music megaton artist unicorn eyeglass crossover Dupont molasses peach
y stupendous
\033[?2004h(kskm) root@coen:/media/HSMFD#
\033[?2004l

Script done on 2024-04-25 21:19:56+00:00 [COMMAND_EXIT_CODE="0"]
```

```
drwxr-xr-x 2 root root 16384 Apr 25 18:39 \033[0m\033[01;34mKSK53-1\033[0m
drwxr-xr-x 3 root root 16384 Apr 25 18:42 \033[01;34mKSK53-2\033[0m

/media/KSRFD/KSK53-1:
total 128
-rw-r--r-- 1 root root 24824 Apr 16 18:27 skr-root-2024-q2-0.xml
-rw-r--r-- 1 root root 11501 Apr 16 18:27 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Apr 16 18:27 ksr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 24832 Apr 25 18:39 skr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 11078 Apr 25 18:39 kskm-ksrsigner-20240425-183615-13267.log

/media/KSRFD/KSK53-2:
total 32
-rw-r--r-- 1 root root 11188 Apr 16 18:27 ksrsigner.yaml
drwxr-xr-x 2 root root 16384 Apr 25 18:39 \033[01;34mKSK53-1\033[0m

/media/KSRFD/KSK53-2/KSK53-1:
total 128
-rw-r--r-- 1 root root 24824 Apr 16 18:27 skr-root-2024-q2-0.xml
-rw-r--r-- 1 root root 11501 Apr 16 18:27 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Apr 16 18:27 ksr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 24832 Apr 25 18:39 skr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 11078 Apr 25 18:39 kskm-ksrsigner-20240425-183615-13267.log
\033[?2004h(kskm) root@coen:/media/HSMFD# diff -qr /media/HSMFD/KSK53-1/ /media/KSRF
\033[?2004h(kskm) root@coen:/media/HSMFD# \033[0K\007\033[0K\007 rm -r KSK53-1/
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK53-2# rm -r KSK53-1/
\033[?2004h(kskm) root@coen:/media/KSRFD/KSK53-2# ls -ltrR
total 16

\033[?2004h(kskm) root@coen:/media/HSMFD# cd /media/HSMFD/
\033[?2004h(kskm) root@coen:/media/HSMFD# cd K\003K\007
KSK29-0-C_to_D/    KSK33-3-C_to_C/    KSK49/
KSK29-1-D_to_C/    KSK35-0-E_to_F/    KSK51/
KSK29-2-C_to_C/    KSK35-1-F_to_G/    KSK53-1/
KSK31-0-D_to_E/    KSK35-2-E_to_E/    KSK53-2/
KSK31-1-E_to_D/    KSK35-3-D_to_D/    KSKSlotDB.config.db
KSK31-2-D_to_D/    KSK37/             KSKSlotDB.db
KSK31-3-C_to_C/    KSK39/             Kjqmt/v.csr
KSK33-0-D_to_E/    KSK43/             Klajeyz.csr
KSK33-1-E_to_D/    KSK45/
KSK33-2-D_to_D/    KSK47/
(kskm) root@coen:/media/HSMFD# cd KSK53-2
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# ls -ltrR

./KSK53-1:
total 24
drwxr-xr-x 2 root root 8192 Apr 25 18:39 \033[0m\033[01;34mKSK53-1\033[0m

./KSK53-1:
total 120
-rw-r--r-- 1 root root 24824 Apr 16 18:27 skr-root-2024-q2-0.xml
-rw-r--r-- 1 root root 11501 Apr 16 18:27 ksrsigner.yaml
-rw-r--r-- 1 root root 19598 Apr 16 18:27 ksr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 24832 Apr 25 18:39 skr-root-2024-q3-0.xml
-rw-r--r-- 1 root root 11078 Apr 25 18:39 kskm-ksrsigner-20240425-183615-13267.log
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# rm -r KSK53-1/
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# ls -ltrR
total 16
-rw-r--r-- 1 root root 11188 Apr 16 18:27 ksrsigner.yaml
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# umount /media/KSRFD/
\033[?2004h(kskm) root@coen:/media/HSMFD/KSK53-2# cd ..
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T18:25:05+0000  ttyUSB0
2024-04-25T18:25:05+0000  ttyUSB0
2024-04-25T18:25:05+0000  ttyUSB0  H2110009 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2024-04-25T18:25:05+0000  ttyUSB0
2024-04-25T18:25:05+0000  ttyUSB0  BBL CRC32: 0xDBC9B9F2
2024-04-25T18:25:05+0000  ttyUSB0  Running applicationBootLoader at 0xEFDC0000
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  H2110009 011403 ABL 030 : Tamper Challenge Response Key
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  ABL CRC32: 0xE7E0FA6A
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  ############################
2024-04-25T18:25:06+0000  ttyUSB0  ###    ABL tamper records    ###
2024-04-25T18:25:06+0000  ttyUSB0  ############################
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  Current Tamper Counts (decimal 0-255):
2024-04-25T18:25:06+0000  ttyUSB0  _____
2024-04-25T18:25:06+0000  ttyUSB0  vextoosTamperCount:        0
2024-04-25T18:25:06+0000  ttyUSB0  vintoosTamperCount:        4
2024-04-25T18:25:06+0000  ttyUSB0  vbboosTamperCount:         0
2024-04-25T18:25:06+0000  ttyUSB0  maxstrtempTamperCount:     0
2024-04-25T18:25:06+0000  ttyUSB0  minstrtempTamperCount:     0
2024-04-25T18:25:06+0000  ttyUSB0  meshTamperCount:           0
2024-04-25T18:25:06+0000  ttyUSB0  extampSMKTamperCount:      0
2024-04-25T18:25:06+0000  ttyUSB0  extampIMKTamperCount:      0
2024-04-25T18:25:06+0000  ttyUSB0  tempdiffTamperCount:       0
2024-04-25T18:25:06+0000  ttyUSB0  pfTamperCount:             4
2024-04-25T18:25:06+0000  ttyUSB0  restartTamperCount::      10
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  Current tamper bitmaps:
2024-04-25T18:25:06+0000  ttyUSB0  _____
2024-04-25T18:25:06+0000  ttyUSB0  currentTamper bitmap:   0x0000  0b .... .... .... ....
2024-04-25T18:25:06+0000  ttyUSB0  lastTamper bitmap:      0x0080  0b .... .... 1.... ....    |EXT_POWER_DOWN
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  Bitmapped Change Record (most recent first):
2024-04-25T18:25:06+0000  ttyUSB0  _____
2024-04-25T18:25:06+0000  ttyUSB0
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T18:25:06+0000  ttyUSB0
2024-04-25T18:25:06+0000  ttyUSB0  Running cryptoApplication at 0xEBF00000
2024-04-25T18:25:07+0000  ttyUSB0
2024-04-25T18:25:07+0000  ttyUSB0  Jumping to startup @ 0x001037B4
2024-04-25T18:25:07+0000  ttyUSB0
2024-04-25T18:25:07+0000  ttyUSB0  Board is P2020RDB
2024-04-25T18:25:07+0000  ttyUSB0
2024-04-25T18:25:07+0000  ttyUSB0  board_smp_init: 2 cpu
2024-04-25T18:25:07+0000  ttyUSB0
2024-04-25T18:25:07+0000  ttyUSB0
2024-04-25T18:25:07+0000  ttyUSB0  Cpu_clk=1000000000, Sys_clk=100000000, CCB=50000000
2024-04-25T18:25:08+0000  ttyUSB0
2024-04-25T18:25:08+0000  ttyUSB0
2024-04-25T18:25:08+0000  ttyUSB0  System page at phys:0000b000 user:0000b000 kern:0000b000
2024-04-25T18:25:08+0000  ttyUSB0  Starting next program at v0015183c
2024-04-25T18:25:08+0000  ttyUSB0
2024-04-25T18:25:08+0000  ttyUSB0  Starting K-Series Kernel
2024-04-25T18:25:08+0000  ttyUSB0
2024-04-25T18:25:08+0000  ttyUSB0  Copyright Ultra Electronics AEP. All Rights Reserved.
2024-04-25T18:25:08+0000  ttyUSB0
2024-04-25T18:25:08+0000  ttyUSB0  Sat Nov 14 04:55:13 1970
2024-04-25T18:25:09+0000  ttyUSB0
2024-04-25T18:25:09+0000  ttyUSB0  Starting auditd v2.0 ... started.
2024-04-25T18:25:09+0000  ttyUSB0
2024-04-25T18:25:09+0000  ttyUSB0  Interface 0 configured for IPv6.
2024-04-25T18:25:09+0000  ttyUSB0
2024-04-25T18:25:09+0000  ttyUSB0  Interface 0 configured for IPv4.
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:10+0000  ttyUSB0  Interface 1 configured for IPv6.
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:10+0000  ttyUSB0  Interface 1 configured for IPv4.
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:10+0000  ttyUSB0  route: writing to routing socket: Network is unreachable
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:10+0000  ttyUSB0  add net default: gateway :::: Network is unreachable
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:10+0000  ttyUSB0  route: writing to routing socket: Network is unreachable
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:10+0000  ttyUSB0  add net default: gateway 0.0.0.0: Network is unreachable
2024-04-25T18:25:10+0000  ttyUSB0
2024-04-25T18:25:11+0000  ttyUSB0  Starting USB driver...
2024-04-25T18:25:11+0000  ttyUSB0
2024-04-25T18:25:11+0000  ttyUSB0  9860 v3.4 Keyper Application - May 19 2017 15:48:58
2024-04-25T18:25:11+0000  ttyUSB0
2024-04-25T18:25:11+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0  Running DES POST Test
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0  DES POST Test Passed
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0  Running Triple DES POST Test
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0  Triple DES POST Test Passed
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0  Running AES POST Test
2024-04-25T18:25:12+0000  ttyUSB0
2024-04-25T18:25:12+0000  ttyUSB0  AES POST Test Passed
2024-04-25T18:25:12+0000  ttyUSB0
```

ttyaudit-ttyUSB0-20240425-182359.log

Timestamp	Port	Message
2024-04-25T18:25:12+0000	ttyUSB0	Running SHA1 POST Test
2024-04-25T18:25:12+0000	ttyUSB0	SHA1 POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running SHA2 POST Test
2024-04-25T18:25:12+0000	ttyUSB0	SHA2 POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running RandomGen POST Test
2024-04-25T18:25:12+0000	ttyUSB0	RandomGen POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running RSA POST Test
2024-04-25T18:25:12+0000	ttyUSB0	RSA POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running DSA POST Test
2024-04-25T18:25:12+0000	ttyUSB0	DSA POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running SEED POST Test
2024-04-25T18:25:12+0000	ttyUSB0	SEED POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running RIPEMD160 POST Test
2024-04-25T18:25:12+0000	ttyUSB0	RIPEMD160 POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running ECC POST Test
2024-04-25T18:25:12+0000	ttyUSB0	ECC POST Test Passed
2024-04-25T18:25:12+0000	ttyUSB0	Running HMAC POST Tests
2024-04-25T18:25:12+0000	ttyUSB0	HMAC POST Tests Passed
2024-04-25T18:25:13+0000	ttyUSB0	Audit on 14/11/1970 04:55:16 00100008
2024-04-25T18:25:13+0000	ttyUSB0	
2024-04-25T18:25:13+0000	ttyUSB0	
2024-04-25T18:25:13+0000	ttyUSB0	
2024-04-25T18:25:13+0000	ttyUSB0	Keyper 9860-2 Serial Number H2110009
2024-04-25T18:25:13+0000	ttyUSB0	
2024-04-25T18:25:13+0000	ttyUSB0	Memory Usage:
2024-04-25T18:25:13+0000	ttyUSB0	RAM (free/total) 192Mb/256Mb
2024-04-25T18:25:13+0000	ttyUSB0	Flash (free/total) 127Mb/128Mb
2024-04-25T18:25:13+0000	ttyUSB0	black store 596b
2024-04-25T18:25:13+0000	ttyUSB0	statistics 112b
2024-04-25T18:25:13+0000	ttyUSB0	other 116b
2024-04-25T18:25:13+0000	ttyUSB0	RedStore (free/total) 107Kb/128Kb
2024-04-25T18:25:13+0000	ttyUSB0	
2024-04-25T18:25:13+0000	ttyUSB0	

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T18:25:13+0000    ttyUSB0 Network Configuration:
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 Interface 0:
2024-04-25T18:25:13+0000    ttyUSB0    IPv4: enabled
2024-04-25T18:25:13+0000    ttyUSB0    IPv6: enabled
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0    MAC/IP address(es): 00:E0:6C:00:C9:4E / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c94e/64
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 Interface 1:
2024-04-25T18:25:13+0000    ttyUSB0    IPv4: enabled
2024-04-25T18:25:13+0000    ttyUSB0    IPv6: enabled
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0    MAC/IP address(es): 00:E0:6C:00:C9:4F / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c94f/64
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 HSM Port 0: 05000
2024-04-25T18:25:13+0000    ttyUSB0 HSM Port 1: 03000
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 Default Gateway(s): 0.0.0.0 ::
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 Software Versions:
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 BBL 030 ABL 021 App 034
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 CPLD Version:
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 1.9
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 SCR Firmware Version:
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 OROS-R2.99-R1.20
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 HmcListener: Created IPv4 socket 12 on port 3000.
2024-04-25T19:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0
2024-04-25T18:25:13+0000    ttyUSB0 HmcListener: Created IPv6 socket 13 on port 3000.
2024-04-25T18:25:14+0000    ttyUSB0
2024-04-25T18:25:14+0000    ttyUSB0 Audit on 14/11/1970 04:55:17 00100003
2024-04-25T18:32:31+0000    ttyUSB0
2024-04-25T18:32:31+0000    ttyUSB0 Audit on 14/11/1970 05:02:35 00200069 4780000D7FAD2972
2024-04-25T18:32:57+0000    ttyUSB0
2024-04-25T18:32:57+0000    ttyUSB0 Audit on 14/11/1970 05:03:01 00200069 3880000D49E32A76
2024-04-25T18:33:33+0000    ttyUSB0
2024-04-25T18:33:33+0000    ttyUSB0 Audit on 14/11/1970 05:03:37 00200069 4780000D7F2D2972
2024-04-25T18:33:35+0000    ttyUSB0
2024-04-25T18:33:35+0000    ttyUSB0 TcpListener: Created IPv4 socket 19 on port 5000.
2024-04-25T18:33:35+0000    ttyUSB0
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T18:33:35+0000  ttyUSB0
2024-04-25T18:33:35+0000  ttyUSB0
2024-04-25T18:33:35+0000  ttyUSB0  TcpListener: Created IPv6 socket 20 on port 5000.
2024-04-25T18:33:35+0000  ttyUSB0
2024-04-25T18:36:16+0000  ttyUSB0  Audit on 14/11/1970 05:03:39 00100002
2024-04-25T18:36:16+0000  ttyUSB0
2024-04-25T18:36:16+0000  ttyUSB0
2024-04-25T18:36:16+0000  ttyUSB0  TcpListener: Accepted connection on socket 21 from address 192.168.0.1.
2024-04-25T18:36:16+0000  ttyUSB0
2024-04-25T18:36:16+0000  ttyUSB0
2024-04-25T18:36:16+0000  ttyUSB0  CryptoTask: Closing connection on socket 21 from address 192.168.0.1.
2024-04-25T18:36:16+0000  ttyUSB0
2024-04-25T18:36:16+0000  ttyUSB0
2024-04-25T18:39:32+0000  ttyUSB0  TcpListener: Accepted connection on socket 23 from address 192.168.0.1.
2024-04-25T18:39:32+0000  ttyUSB0
2024-04-25T18:39:32+0000  ttyUSB0
2024-04-25T18:39:32+0000  ttyUSB0  CryptoTask: Closing connection on socket 23 from address 192.168.0.1.
2024-04-25T18:52:22+0000  ttyUSB0
2024-04-25T18:52:22+0000  ttyUSB0  Audit on 14/11/1970 05:22:26 00200069 388000D049E32A76
2024-04-25T18:52:48+0000  ttyUSB0
2024-04-25T18:52:48+0000  ttyUSB0  Audit on 14/11/1970 05:22:52 00200069 478000007F2D2972
2024-04-25T18:53:12+0000  ttyUSB0
2024-04-25T18:53:12+0000  ttyUSB0  Audit on 14/11/1970 05:23:16 00200069 478000007FAD2972
2024-04-25T18:53:16+0000  ttyUSB0
2024-04-25T18:53:16+0000  ttyUSB0
2024-04-25T18:53:16+0000  ttyUSB0  TcpListener: Closed IPv4 socket 19 on port 5000.
2024-04-25T18:53:16+0000  ttyUSB0
2024-04-25T18:53:16+0000  ttyUSB0
2024-04-25T18:53:16+0000  ttyUSB0  TcpListener: Closed IPv6 socket 20 on port 5000.
2024-04-25T18:53:16+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  Audit on 14/11/1970 05:23:20 00100003
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  H1903018 011397 BBL 030 : Factory Software Verification Key : CPLD version 1.9 : Hardware revision 2870-G2
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  BBL CRC32: 0xDBC9B9F2
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  Running applicationBootLoader at 0xEFDC0000
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  H1903018 011403 ABL 030 : Tamper Challenge Response Key
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  ABL CRC32: 0xE7E0FA6A
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  *******************************************
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  ***    ABL tamper records    ***
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  *******************************************
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  Current Tamper Counts (decimal 0-255):
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0  _____
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T19:18:49+0000  ttyUSB0 vextoosTamperCount:      0
2024-04-25T19:18:49+0000  ttyUSB0 vintoosTamperCount:      9
2024-04-25T19:18:49+0000  ttyUSB0 vbboosTamperCount:       0
2024-04-25T19:18:49+0000  ttyUSB0 maxstrtempTamperCount:   0
2024-04-25T19:18:49+0000  ttyUSB0 minstrtempTamperCount:   0
2024-04-25T19:18:49+0000  ttyUSB0 meshTamperCount:         0
2024-04-25T19:18:49+0000  ttyUSB0 extampSYKTamperCount:    0
2024-04-25T19:18:49+0000  ttyUSB0 extanpIMKTamperCount:    0
2024-04-25T19:18:49+0000  ttyUSB0 tempdiffTamperCount:     0
2024-04-25T19:18:49+0000  ttyUSB0 pfTamperCount:           9
2024-04-25T19:18:49+0000  ttyUSB0 restartTamperCount:      31
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0 Current tamper bitmaps:
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0 currentTamper bitmap:  0x0000  0b .... .... .... ....
2024-04-25T19:18:49+0000  ttyUSB0 lastTamper bitmap:     0x0080  0b .... .... 1... .... |EXT_POWER_DOWN
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0 Bitmapped Change Record (most recent first):
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:49+0000  ttyUSB0
2024-04-25T19:18:51+0000  ttyUSB0 Running cryptoApplication at 0xEHF00000
2024-04-25T19:18:51+0000  ttyUSB0 Jumping to startup @ 0x001037B4
2024-04-25T19:18:51+0000  ttyUSB0 Board is P2020RDB
2024-04-25T19:18:51+0000  ttyUSB0 board_smp_init: 2 cpu
2024-04-25T19:18:51+0000  ttyUSB0
2024-04-25T19:18:51+0000  ttyUSB0 Cpu_clk-1000000000, Sys_clk=100000000, CCB=500000000
2024-04-25T19:18:52+0000  ttyUSB0 System page at phys:0000b000 user:0000b000 kern:0000b000
2024-04-25T19:18:52+0000  ttyUSB0 Starting next program at v0015183c
2024-04-25T19:18:52+0000  ttyUSB0 Starting K-Series Kernel
2024-04-25T19:18:52+0000  ttyUSB0 Copyright Ultra Electronics AEP. All Rights Reserved.
2024-04-25T19:18:52+0000  ttyUSB0 Sat Jan 11 03:26:43 1975
2024-04-25T19:18:52+0000  ttyUSB0
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T19:18:52+0000  ttyUSB0  Starting auditd v2.0 ... started.
2024-04-25T19:18:52+0000  ttyUSB0
2024-04-25T19:18:53+0000  ttyUSB0  Interface 0 configured for IPv6.
2024-04-25T19:18:53+0000  ttyUSB0
2024-04-25T19:18:53+0000  ttyUSB0  Interface 0 configured for IPv4.
2024-04-25T19:18:53+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  Interface 1 configured for IPv6.
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  Interface 1 configured for IPv4.
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  route: writing to routing socket: Network is unreachable
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  add net default: gateway ::: Network is unreachable
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  route: writing to routing socket: Network is unreachable
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  add net default: gateway 0.0.0.0: Network is unreachable
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  Starting USB driver...
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:54+0000  ttyUSB0  9860 v3.4 Keyper Application - May 19 2017 15:48:58
2024-04-25T19:18:54+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running DES POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  DES POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running Triple DES POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Triple DES POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running AES POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  AES POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running SHA1 POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  SHA1 POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running SHA2 POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  SHA2 POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running RandomGen POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  RandomGen POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running RSA POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  RSA POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running DSA POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  DSA POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running SEED POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  SEED POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running RIPEMD160 POST Test
2024-04-25T19:18:56+0000  ttyUSB0
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T19:18:56+0000  ttyUSB0  RIPEMD160 POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running ECC POST Test
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  ECC POST Test Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Running HMAC POST Tests
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  HMAC POST Tests Passed
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0  Audit on 11/1/1975 03:26:47 00100008
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:56+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  Keyper 9960-2  Serial Number H1903018
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  Memory Usage:
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  RAM (free/total)         192Mb/256Mb
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  Flash (free/total)       127Mb/128Mb
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     Black store           596b
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     statistics            112b
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     other                 1:6b
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  RedStore (free/total)    107Kb/128Kb
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  Network Configuration:
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  Interface 0:
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     IPv4: enabled
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     IPv6: enabled
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C4:9D / 192.168.0.2/24 , 2001::2e0:6cff:fe00:c49d/64
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  Interface 1:
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     IPv4: enabled
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     IPv6: enabled
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0     MAC/IP address(es): 00:E0:6C:00:C4:9E / 192.168.1.2/24 , 2001::1:2e0:6cff:fe00:c49e/64
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0  HSM Port 0: 05000
2024-04-25T19:18:57+0000  ttyUSB0  HSM Port 1: 03000
2024-04-25T19:18:57+0000  ttyUSB0  Default Gateway(s): 0.0.0.0 ::
2024-04-25T19:18:57+0000  ttyUSB0
2024-04-25T19:18:57+0000  ttyUSB0
```

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T19:18:57+0000    ttyUSB0   Software Versions:
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   BBL 030 ABL 021 App 034
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   CPLD Version:
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   1.9
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   SCR Firmware Version:
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   OROS-R2.99-R1.20
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   HmcListener: Created IPv4 socket 12 on port 3000.
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:18:57+0000    ttyUSB0   HmcListener: Created IPv6 socket 13 on port 3000.
2024-04-25T19:18:57+0000    ttyUSB0
2024-04-25T19:44:34+0000    ttyUSB0   Audit on 11/1/1975 03:26:47 00100003
2024-04-25T19:44:34+0000    ttyUSB0
2024-04-25T19:44:58+0000    ttyUSB0   Audit on 11/1/1975 03:52:24 0020006b 4780000094AD2972
2024-04-25T19:44:58+0000    ttyUSB0
2024-04-25T19:45:24+0000    ttyUSB0   Audit on 11/1/1975 03:52:49 0020006b 4780000080ED2972
2024-04-25T19:45:24+0000    ttyUSB0
2024-04-25T19:45:24+0000    ttyUSB0   Audit on 11/1/1975 03:53:15 0020006b 4780000952D2972
2024-04-25T19:45:43+0000    ttyUSB0
2024-04-25T19:45:43+0000    ttyUSB0
2024-04-25T19:45:43+0000    ttyUSB0   _____
2024-04-25T19:45:43+0000    ttyUSB0   Key Details
2024-04-25T19:45:43+0000    ttyUSB0   _____
2024-04-25T19:45:43+0000    ttyUSB0   Klajeyz,RSA,FIPS,2048,wt,svedmvu
2024-04-25T19:45:43+0000    ttyUSB0
2024-04-25T19:45:43+0000    ttyUSB0   Kmrf13b,RSA,FIPS,2048,wt,sd
2024-04-25T19:45:43+0000    ttyUSB0
2024-04-25T19:45:43+0000    ttyUSB0   _____
2024-04-25T19:45:43+0000    ttyUSB0
2024-04-25T19:45:48+0000    ttyUSB0
2024-04-25T19:45:48+0000    ttyUSB0   _____
2024-04-25T19:45:48+0000    ttyUSB0
2024-04-25T19:45:48+0000    ttyUSB0   Key Summary
2024-04-25T19:45:48+0000    ttyUSB0
2024-04-25T19:45:48+0000    ttyUSB0   RSA,2048,Private,2
2024-04-25T19:45:48+0000    ttyUSB0
2024-04-25T19:45:48+0000    ttyUSB0   _____
2024-04-25T19:45:48+0000    ttyUSB0
2024-04-25T19:45:48+0000    ttyUSB0
```

04/25/24
20:29:58

ttyaudit-ttyUSB0-20240425-182359.log

```
2024-04-25T19:47:48+0000   ttyUSB0 Audit on 11/1/1975 03:55:38 0020004f Kmrf13b
2024-04-25T19:47:48+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0 Key Details
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0 Klajeyz,RSA,FIPS,2048,wL,svedmvu
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:23+0000   ttyUSB0
2024-04-25T19:48:27+0000   ttyUSB0
2024-04-25T19:48:27+0000   ttyUSB0 Key Summary
2024-04-25T19:48:28+0000   ttyUSB0
2024-04-25T19:48:28+0000   ttyUSB0 RSA,2048,Private,1
2024-04-25T19:48:28+0000   ttyUSB0
2024-04-25T19:48:28+0000   ttyUSB0
2024-04-25T19:48:28+0000   ttyUSB0 Audit on 11/1/1975 03:57:01 0020001c
2024-04-25T19:48:28+0000   ttyUSB0
2024-04-25T19:48:28+0000   ttyUSB0 Audit on 11/1/1975 03:58:57 00200014 3F400031F88A2A77; 120D
2024-04-25T19:48:28+0000   ttyUSB0
2024-04-25T19:48:28+0000   ttyUSB0
2024-04-25T19:49:11+0000   ttyUSB0
2024-04-25T19:49:11+0000   ttyUSB0 Key Details
2024-04-25T19:51:07+0000   ttyUSB0
2024-04-25T19:51:07+0000   ttyUSB0 Klajeyz,RSA,FIPS,2048,wL,svedmvu
2024-04-25T19:51:44+0000   ttyUSB0
2024-04-25T19:51:44+0000   ttyUSB0
2024-04-25T19:51:44+0000   ttyUSB0
2024-04-25T19:51:44+0000   ttyUSB0 Key Summary
2024-04-25T19:51:44+0000   ttyUSB0
2024-04-25T19:51:44+0000   ttyUSB0 RSA,2048,Private,1
2024-04-25T19:51:44+0000   ttyUSB0
2024-04-25T19:51:44+0000   ttyUSB0
2024-04-25T19:51:47+0000   ttyUSB0 Audit on 11/1/1975 04:01:46 00200025 00800002710F156D
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:51:48+0000   ttyUSB0
2024-04-25T19:53:56+0000   ttyUSB0
2024-04-25T19:53:56+0000   ttyUSB0
```

04/25/24
20:29:58

ttyaudit-ttyUSB0-20240425-182359.log

2024-04-25T19:54:28+0000   ttyUSB0   Audit on 11/1/1975 04:02:19 00200025 008000002928F156D
2024-04-25T19:54:28+0000   ttyUSB0
2024-04-25T19:54:53+0000   ttyUSB0   Audit on 11/1/1975 04:02:44 00200025 0880004A79F3296D
2024-04-25T19:54:53+0000   ttyUSB0
2024-04-25T19:55:17+0000   ttyUSB0   Audit on 11/1/1975 04:03:07 00200025 008000277CF156D
2024-04-25T19:55:17+0000   ttyUSB0
2024-04-25T19:55:41+0000   ttyUSB0   Audit on 11/1/1975 04:03:32 00200025 008000029E8F156D
2024-04-25T19:55:41+0000   ttyUSB0
2024-04-25T19:55:44+0000   ttyUSB0   Audit on 11/1/1975 04:03:35 00200005
2024-04-25T19:55:44+0000   ttyUSB0
2024-04-25T19:57:05+0000   ttyUSB0   Audit on 11/1/1975 04:04:55 00200016 Kmrfl3b
2024-04-25T19:57:05+0000   ttyUSB0
2024-04-25T19:57:05+0000   ttyUSB0   Audit on 11/1/1975 04:04:55 00200015 3F4C0031F88A2A77
2024-04-25T19:57:05+0000   ttyUSB0
2024-04-25T19:57:05+0000   ttyUSB0   Audit on 11/1/1975 04:04:55 00200018
2024-04-25T19:57:32+0000   ttyUSB0
2024-04-25T19:57:32+0000   ttyUSB0
2024-04-25T19:57:32+0000   ttyUSB0   Key Details
2024-04-25T19:57:32+0000   ttyUSB0
2024-04-25T19:57:32+0000   ttyUSB0   Klajeyz,RSA,FIPS,2048,wt,svedmvu
2024-04-25T19:57:32+0000   ttyUSB0
2024-04-25T19:57:32+0000   ttyUSB0   Kmrfl3b,RSA,FIPS,2048,wt,sd
2024-04-25T19:57:32+0000   ttyUSB0
2024-04-25T19:57:32+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0   Key Summary
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0   RSA,2048,Private,2
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T19:57:39+0000   ttyUSB0
2024-04-25T20:03:54+0000   ttyUSB0   Audit on 11/1/1975 04:11:45 0020002d 3F4C0033C8CA2A77
2024-04-25T20:03:54+0000   ttyUSB0
2024-04-25T20:04:36+0000   ttyUSB0   Audit on 11/1/1975 04:12:27 0020002d 3F4C0031D60A2A77
2024-04-25T20:04:36+0000   ttyUSB0
2024-04-25T20:05:19+0000   ttyUSB0   Audit on 11/1/1975 04:13:09 0020002d 3F4C0031D68A2A77
2024-04-25T20:05:19+0000   ttyUSB0
2024-04-25T20:06:05+0000   ttyUSB0   Audit on 11/1/1975 04:13:55 0020002d 3F4C0335F8A2A77
2024-04-25T20:06:05+0000   ttyUSB0
2024-04-25T20:06:48+0000   ttyUSB0   Audit on 11/1/1975 04:14:39 0020002d 3F4C0033690A2A77
2024-04-25T20:06:48+0000   ttyUSB0
2024-04-25T20:07:40+0000   ttyUSB0   Audit on 11/1/1975 04:15:30 0020002d 3F4C0335CCA2A77
2024-04-25T20:08:26+0000   ttyUSB0   Audit on 11/1/1975 04:16:16 0020002d 3F4C0033624A2A77
2024-04-25T20:09:26+0000   ttyUSB0
2024-04-25T20:10:51+0000   ttyUSB0   Audit on 11/1/1975 04:18:42 00200007
2024-04-25T20:11:40+0000   ttyUSB0   Audit on 11/1/1975 04:19:29 0020002d 3F4C0033C84A2A77
2024-04-25T20:11:40+0000   ttyUSB0

ttyaudit-ttyUSB0-20240425-182359.log

04/25/24
20:29:58

```
2024-04-25T20:12:21+0000   ttyUSB0 Audit on 11/1/1975 04:20:12 0020002d 3F40003D64A2A77
2024-04-25T20:12:21+0000   ttyUSB0
2024-04-25T20:12:59+0000   ttyUSB0 Audit on 11/1/1975 04:20:50 0020002d 3F40003335ECA2A77
2024-04-25T20:12:59+0000   ttyUSB0
2024-04-25T20:13:41+0000   ttyUSB0 Audit on 11/1/1975 04:21:31 0020002d 3F40003B68A2A77
2024-04-25T20:13:41+0000   ttyUSB0
2024-04-25T20:14:21+0000   ttyUSB0 Audit on 11/1/1975 04:22:11 0020002d 3F40003335C8A2A77
2024-04-25T20:14:21+0000   ttyUSB0
2024-04-25T20:15:04+0000   ttyUSB0 Audit on 11/1/1975 04:22:55 0020002d 3F40003350DA2A77
2024-04-25T20:15:04+0000   ttyUSB0
2024-04-25T20:15:42+0000   ttyUSB0 Audit on 11/1/1975 04:23:32 0020002d 3F40003350D4A2A77
2024-04-25T20:15:42+0000   ttyUSB0
2024-04-25T20:17:52+0000   ttyUSB0 Audit on 11/1/1975 04:25:42 00200007
2024-04-25T20:17:52+0000   ttyUSB0
2024-04-25T20:20:18+0000   ttyUSB0 Audit on 11/1/1975 04:28:09 0020002d 0880004A79F3296D
2024-04-25T20:20:18+0000   ttyUSB0
2024-04-25T20:20:52+0000   ttyUSB0 Audit on 11/1/1975 04:28:43 0020002d 08000029E8F156D
2024-04-25T20:20:52+0000   ttyUSB0
2024-04-25T20:21:28+0000   ttyUSB0 Audit on 11/1/1975 04:29:19 0020002d 080000029C4F156D
2024-04-25T20:21:28+0000   ttyUSB0
2024-04-25T20:22:06+0000   ttyUSB0 Audit on 11/1/1975 04:29:56 0020002d 00900002710F156D
2024-04-25T20:22:06+0000   ttyUSB0
2024-04-25T20:22:44+0000   ttyUSB0 Audit on 11/1/1975 04:30:34 0020002d 008000002928F156D
2024-04-25T20:22:44+0000   ttyUSB0
2024-04-25T20:23:22+0000   ttyUSB0 Audit on 11/1/1975 04:31:12 0020002d 0090000277CF156D
2024-04-25T20:23:22+0000   ttyUSB0
2024-04-25T20:25:02+0000   ttyUSB0 Audit on 11/1/1975 04:32:52 0020002d 0880004A7C73296D
2024-04-25T20:25:02+0000   ttyUSB0
2024-04-25T20:27:33+0000   ttyUSB0 Audit on 11/1/1975 04:35:24 0020002d 00400017B9A0E6C
2024-04-25T20:27:33+0000   ttyUSB0
2024-04-25T20:28:12+0000   ttyUSB0 Audit on 11/1/1975 04:36:02 0020002d 008000028F8F156D
2024-04-25T20:28:12+0000   ttyUSB0
2024-04-25T20:28:48+0000   ttyUSB0 Audit on 11/1/1975 04:36:38 0020002d 008000028F4F156D
2024-04-25T20:28:48+0000   ttyUSB0
2024-04-25T20:29:21+0000   ttyUSB0 Audit on 11/1/1975 04:37:12 0020002d 008000029D0F156D
2024-04-25T20:29:21+0000   ttyUSB0
2024-04-25T20:29:59+0000   ttyUSB0 Audit on 11/1/1975 04:37:49 0020002d 008000028FCF156D
2024-04-25T20:29:59+0000   ttyUSB0
```

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

SHA-256:   01cf6b152bf1f5c8dfc9dfef0b3c06b2e7eba689abc3709c059542892e6f6fe0
PGP Words: absurd Saturday glitter bifocals briefcase vacancy vapor retrieval talon retros
pect talon unravel alone crossover afflict pioneer transit underfoot rematch matchmaker rhy
thm replica guidance October adult Montana crowfoot matchmaker buzzard hemisphere gremlin t
obacco

Act 6: Secure Hardware

The CA will secure the ceremony hardware to prepare it for storage by performing the steps below:

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

Stop Logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
6.1	CA performs the following steps to stop logging: a) Perform the following steps using the **HSM Output** terminal window to stop logging the serial output **(ttyaudit)**: 　i) Press `Ctrl + C` 　ii) Execute `exit` b) Execute the command below using the **Commands** terminal window to stop logging the terminal session: `exit` Note: The Commands terminal session window will remain open. c) Disconnect the null modem and ethernet cables from the laptop.	_M_	21:20

Print Logging Information

Step	Activity	Initials	Time
6.2	CA executes the following commands to print a copy of the logging information: a) `print-script script-202404*.log` b) `print-ttyaudit ttyaudit-tty*-202404*.log` Attach the printed copies to IW script. Note: Ignore the error regarding non-printable characters if prompted.	_M_	21:26

Prepare Blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
6.3	CA executes the following command to print **two** copies of the hash for the HSMFD content: `hsmfd-hash -p` Note: One copy for the audit bundle and one copy for the OS media TEB.	_M_	21:27
6.4	CA executes the command below to display the contents of the HSMFD: `ls -ltrR`	_M_	21:27
6.5	CA executes the command below and follows the interactive prompts in the terminal window to create **five** HSMFDs copies: `copy-hsmfd` Note 1: Wait for the activity light on the copied HSMFD to stop flashing before removal. Note 2: "copy-hsmfd -v" can be used to activate verbose mode.	_M_	21:34

Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
6.6	Using the **Commands** terminal window, CA executes the commands below to unmount the HSMFD: a) `cd /tmp` b) `umount /media/HSMFD` CA removes the HSMFD, then places it on the holder. Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.	_M_	21:34
6.7	CA performs the following steps to shut down the laptop: a) Power **OFF** the laptop by pressing the power button. b) Disconnect all connections from the laptop. c) Remove the OS media from the laptop, and place it in its case. d) Close all laptop latches.	_M_	21:35
6.8	CA performs the following steps to prepare the OS media bundle for storage: a) Ask the IW for the OS media bundle's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Place 2 HSMFDs and 2 OS media SD cards into a plastic card case. c) Place the plastic card case containing 2 HSMFDs and 2 OS media SD cards along with 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS media bundle onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the OS media bundle TEB on the cart. **OS Media (release coen-1.1.0) + HSMFD: TEB # BB02639666**	_M_	21:37
6.9	CA distributes the following HSMFDs: 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review).	_M_	21:38

Place Laptop3 into a TEB

Step	Activity	Initials	Time
6.10	CA performs the following steps to prepare the Laptop for storage: a) Ask the IW for the Laptop's designated new TEB, then read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the service tag number from the bottom of the laptop while the IW verifies it matches the information below. c) Place the Laptop into its designated new TEB, then seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the Laptop onto the HSM designated space of the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the Laptop TEB on the cart. **Laptop3: TEB # BB81420051 / Service Tag # J8SVSG2**	_M_	21:40

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
6.11	The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps: a) CA asks the IW for the CO's designated new TEB, then reads the TEB number and description aloud while IW verifies it matches the information below. b) CO removes their credentials from the card holder, then hands them to the CA. c) CA verifies the credentials, then places them into an available plastic case. d) CA places the plastic case into its designated new TEB, then seals it. e) CA gives the IW sealing strips for post-ceremony inventory. f) CA places the TEB onto the HSM designated space of the ceremony table visible to the audit camera. g) CA initials the TEB with a ballpoint pen. h) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. i) CA gives the TEB containing the cards to the CO. j) CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen. k) CO writes the date and time, signs the credential table of the IW's script, then the IW initials the entry. l) CO returns to their seat with their TEBs. m) Repeat steps for all the remaining COs' credentials on the list. **CO2: Pia Gruvö** **Set # 2 TEB # BB02639669** **CO4: Robert Seastrom** **Set # 2 TEB # BB02639668** **CO7: Dileepa Lathsara** **Set # 2 TEB # BB02639667**	*M*	21:46

Act 6: Secure Hardware

TCR	TEB #	Printed Name	Signature	Date	Time	IW Initials
CO2	Set # 2 TEB # BB02639669	Pia Gruvö		2024 Apr 25	21:42	
CO4	Set # 2 TEB # BB02639668	Robert Seastrom		2024 Apr 25	21:44	
CO7	Set # 2 TEB # BB02639667	Dileepa Lathsara		2024 Apr 25	21:46	

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

Step	Activity	Initials	Time
6.12	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)	*Ch*	21:48
6.13	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.	*ar*	21:48
6.14	SSC1 removes the safe log, 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.	*M*	21:49
6.15	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, then verify its integrity. c) Present the equipment TEB to the audit camera above, then place it inside Safe #1 (Equipment Safe). d) Write the date, time, and signature on the safe log where **"Return"** is indicated. e) IW verifies the safe log entry, then initials it. **HSM5E: TEB # BB51184554** **HSM7E: TEB # BB51184553** **Laptop3: TEB # BB81420051** **OS media (release coen-1.1.0) + HSMFD: TEB # BB02639666** **KSK-2023: TEB # BB02639665** Note: The shelves in the equipment safe can slide in and out for ease of use.	*M*	21:52

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
6.16	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.	*M*	21:53
6.17	SSC1 returns the safe log to Safe #1, closes the safe door, pulls up on the handle, then 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 adjacent to the Tier 5 (Safe Room) exit door is off.	*M*	21:53
6.18	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).	*M*	21:54

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
6.19	CA transports the guard key and a flashlight, and with IW escort SSC2 and the COs into Tier 5 (Safe Room.)	*M*	21:54
6.20	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.	*M*	21:56
6.21	SSC2 removes the safe log, 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.	*M*	21:57

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

Step	Activity	Initials	Time
6.22	COs perform the following steps sequentially to return the listed TEBs: a) CO reads aloud the TEB number, verifies integrity of TEB, then presents it to the audit camera above. b) CO announces their box number, then CA operates the guard key in that box's lower lock with the key blade facing downward. c) CO operates their tenant key in that box's upper lock with the key blade facing upward, then opens the safe deposit box. d) CO places their TEB(s) in their safe deposit box, locks it, then removes their key. e) CO writes the date and time, then signs the safe log where **"Return"** is indicated. f) IW verifies the completed safe log entry, then initials it. g) CA locks the safe deposit box, then removes the guard key. **CO2: Pia Gruvö** **Box # 1264** **Set # 2 TEB # BB02639669** **CO4: Robert Seastrom** **Box # 1243** **Set # 2 TEB # BB02639668** **CO7: Dileepa Lathsara** **Box # 1263** **Set # 2 TEB # BB02639667**	_M_	22:01

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
6.23	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.	_M_	22:02
6.24	SSC2 returns the safe log to Safe #2, closes the safe door, pulls up on the handle, then 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 adjacent to the Tier 5 (Safe Room) exit door is off.	_M_	22:02
6.25	CA, IW, SSC2, and COs leave Tier 5 (Safe Room) returning to Tier 4 (Key Ceremony Room).	_M_	22:03

Act 7: Close the Key Signing Ceremony

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

- Read any exceptions that occurred during the ceremony
- Call the ceremony participants to sign the IW's script
- Stop the online streaming and video recording

Participants Sign IW's Script

Step	Activity	Initials	Time
7.1	CA reads all exceptions that occurred during the ceremony.	_(initials)_	22:07
7.2	CA calls each in-person attendee not seated at the ceremony table to sign the IW's participant list. **All signatories declare to the best of their knowledge that this script is a true and accurate record of the ceremony.**	_(initials)_	22:11
7.3	CA reviews IW's script, then signs the participants list.	_(initials)_	22:13
7.4	IW signs the list and records the completion time.	_(initials)_	22:14

Stop Online Streaming and Recording

Step	Activity	Initials	Time
7.5	CA acknowledges the participation of the online participants, then instructs the SA to stop the online streaming.	_(initials)_	22:14
7.6	CA instructs the SA to stop the audit camera video recording.	_(initials)_	22:14
7.7	CA informs onsite participants of post ceremony activities.	_(initials)_	22:15
7.8	Ceremony participants take a group photo.	_(initials)_	22:15

Appendix A: Glossary

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

    https://github.com/iana-org/coen

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

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

[4] **hsmfd-hash:*** A bash script used to calculate, print, and compare SHA-256 checksums for the HSMFD flash drives.
    Note: The sort command has different behavior depending on the locale settings specified by environment variables. Current OS locale setting is LC_COLLATE="POSIX"

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

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

[7] **ksrsigner:** A legacy application that uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.

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

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

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

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

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

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

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

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

---

* The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-1.1.0coen_amd64.deb
A debian package is an **ar** archive. To extract data from a deb package, use the command **ar -x ksk-tools-1.1.0coen_amd64.deb**
Then extract the files with **tar -xvf data.tar.xz**
The file will be located in the directory: **./opt/icann/bin/**
** The source code is available at https://github.com/iana-org/dnssec-keytools

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

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

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

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

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

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

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

[15] **Thales Luna HSM Role iKeys:**

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

    b) **SO (Security Officer):** Required for administration of the HSMs.

    c) **Audit:** Required to access transaction logs from the HSMs.

    d) **Domain:** Associates HSMs to facilitate cloning key materials to dedicated Luna backup HSMs.

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes generated during the ceremony, and attestation. See Appendix C on page 43.

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 44.

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

7. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 53-1**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

Appendix C: Key Ceremony Script (by IW)

I hereby attest that the Key Ceremony was conducted in accordance with this script.
Any exceptions that occurred were accurately and properly documented.

IW: **Andy Newton**

Signature:

Date: 2024 Apr ___

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: **20231130 00:00:00 to 20240426 00:00:00 UTC.**

SA: Darren Kara

Signature:

Date: 2024 Apr 25

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 7th Edition (2024-03-15). No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA: Darren Kara

Signature:

Date: 2024 Apr 25