

# **Root DNSSEC KSK Ceremony 51**

Thursday 30 November 2023

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

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

## Abbreviations

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

## Participants

Key Ceremony roles are described on <https://www.iana.org/help/key-ceremony-roles>

**Instructions:** At the end of the ceremony, participants sign IW's script. IW records time of completion.

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

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

## Instructions for a Root DNSSEC KSK Ceremony

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

### Ceremony Guidelines:

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

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

### Key Management Facility Tiers:

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

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

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

# Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

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

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

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

## Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.		
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.		
3	CA asks that any first time ceremony participants in the room introduce themselves.		

## Emergency Evacuation Procedures and Electronics Policy

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

## Verify the Time and Date

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

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

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

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

Step	Activity	Initials	Time
11	<p>COs perform the following steps sequentially to access the listed TEBs:</p> <ul style="list-style-type: none"> <li>a) After the CA operates the guard key in the bottom lock, CO reads aloud their safe deposit box number then uses their tenant key to operate the top lock.</li> <li>b) CO opens their safe deposit box, verifies its integrity, then removes the TEBs.</li> <li>c) CO reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above.</li> <li>d) CO performs the actions specified below, then locks their safe deposit box.</li> </ul> <p><b>Note 1:</b> The CO's key will remain inserted in their assigned safe deposit box lock when specified below.</p> <p><b>Note 2:</b> The COs will retrieve their new safe deposit box keys when specified below.</p> <ul style="list-style-type: none"> <li>e) CO writes the date and time, then signs the safe log.</li> <li>f) IW verifies the completed safe log entries, then initials them.</li> </ul> <p><b>CO1: Frederico Neves</b>  <b>Box # 1239</b>  <b>Set # 1 TEB # BB02639501</b> (Retain)                      Last Verified: KSK Ceremony 47 2022-11-03  <b>Set # 2 TEB # BB02638534</b> (Check and Return)                      Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>CO2: Pia Gruvö</b>  <b>Box # 1264</b>  <b>Set # 1 TEB # BB02639500</b> (Retain)                      Last Verified: KSK Ceremony 47 2022-11-03  <b>Set # 2 TEB # BB02639498</b> (Check and Return)                      Last Verified: KSK Ceremony 45 2022-05-12</p> <p><b>CO4: Robert Seastrom</b>  <b>Box # 1260</b> (Key shall remain in lock)  <b>New Box # 1243</b> (Retrieve keys from lock)  <b>OP TEB # BB91951237</b> (Retain)  <b>SO TEB # BB02639553</b> (Retain)  <b>Set # 1 TEB # BB02639552</b> (Retain)                      Last Verified: KSK Ceremony 45 2022-05-12  <b>Set # 2 TEB # BB02639551</b> (Transfer to newly assigned safe deposit box)                      Last Verified: KSK Ceremony 45 2022-05-12</p> <p><b>CO5: Nomsa Mwayenga</b>  <b>Box # 1262</b>  <b>Set # 1 TEB # BB02639496</b> (Retain)                      Last Verified: KSK Ceremony 47 2022-11-03  <b>Set # 2 TEB # BB02639548</b> (Retain)                      Last Verified: KSK Ceremony 45 2022-05-12</p> <p><b>CO6: Hugo Salgado</b>  <b>Box # 1242</b>  <b>Set # 1 TEB # BB02638531</b> (Retain)                      Last Verified: KSK Ceremony 49 2023-04-27  <b>Set # 2 TEB # BB02638530</b> (Check and Return)                      Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Note:</b> "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		

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

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

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

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



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

Step	Activity	Initials	Time
18	<p>CA performs the following steps to extract each piece of equipment from the safe:</p> <ul style="list-style-type: none"> <li>a) CAREFULLY remove each equipment TEB from the safe.</li> <li>b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera.</li> <li>c) Place each equipment TEB on the cart as specified in the list below.</li> <li>d) Write the date and time, then signs the safe log.</li> <li>e) IW verifies the completed safe log entries, then initials it.</li> </ul> <p><b>HSM5E: TEB # BB51184606 (Place on Cart)</b> Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>HSM6E: TEB # BB51184243 (Check and Return)</b> Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>HSM7E: TEB # BB51184253 (Place on Cart)</b> Last Verified: AT Ceremony 51 2023-11-29</p> <p><b>HSM8E: TEB # BB51184254 (Place on Cart)</b> Last Verified: AT Ceremony 51 2023-11-29</p> <p><b>Laptop3: TEB # BB97448418 (Check and Return)</b> Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Laptop4: TEB # BB81420064 (Place on Cart)</b> Last Verified: KSK Ceremony 47 2022-11-03</p> <p><b>OS media (release coen-1.0.0) + HSMFD: TEB # BB02638528 (Place on Cart)</b> Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>KSK-2017: TEB # BB46584614 (Place on Cart)</b> Last Verified: KSK Ceremony 43 2021-10-14</p> <p><b>KSK-2023: TEB # BB02638526 (Place on Cart)</b> Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</b></p>		

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

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

# Act 2: Equipment Setup

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

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

## Laptop Setup

Step	Activity	Initials	Time
1	<p>CA performs the following steps to prepare the listed equipment:</p> <ol style="list-style-type: none"> <li>a) Remove all equipment TEBs from the cart and place them on the ceremony table.</li> <li>b) Inspect each equipment TEB for tamper evidence.</li> <li>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.</li> <li>d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.</li> </ol> <p><b>HSM5E: TEB # BB51184606 / Serial # H1903018</b>                      Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Laptop4: TEB # BB81420064 / Service Tag # 58SVSG2</b>                      Last Verified: KSK Ceremony 47 2022-11-03</p> <p><b>OS media (release coen-1.0.0) + HSMFD: TEB # BB02638528</b>                      Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</b></p>		
2	<p>CA performs the following steps to confirm that no hard drive and battery are in the laptop:</p> <ol style="list-style-type: none"> <li>a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty.</li> <li>b) Open the latch on the left side of the laptop to confirm that the battery slot is empty.</li> </ol>		
3	<p>CA ensures the <b>lock switch</b> on the left side of the listed SD card is slid down to the lock position:  <b>OS media release coen-1.0.0</b>  <b>Copy # 2</b></p>		
4	<p>CA performs the following steps to boot the laptop:</p> <ol style="list-style-type: none"> <li>a) Connect the USB printer cable into the rear USB port of the laptop.</li> <li>b) Connect the null modem cable into a USB port of the laptop.</li> <li>c) Connect the external HDMI display cable.</li> <li>d) Connect the power supply.</li> <li>e) Insert the <b>OS media release coen-1.0.0 Copy # 2</b>.</li> <li>f) Switch it ON.</li> </ol>		
5	<p>CA verifies functionality of the external display and performs adjustments if necessary:                      To change the font size of the terminal:                      Click the <b>View</b> menu and select <b>Zoom In</b> or <b>Zoom Out</b>                      To change the resolution of each screen:                      Go to <b>Applications &gt; Settings &gt; Display</b></p>		

## OS Media Checksum Verification

Step	Activity	Initials	Time
6	<p>CA uses the terminal window to executes the following steps:</p> <ul style="list-style-type: none"> <li>a) Verify the byte count of the SD card matches the ISO size of by running the following command: <code>df -B1 /dev/sda</code></li> <li>b) Calculate the SHA-256 hash by executing: <code>head -c 375431168 /dev/sda   sha2wordlist</code></li> <li>c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.</li> </ul> <p>Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.</p> <p>SHA-256 hash: 405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a</p> <p>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</p> <p>Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website <a href="https://www.iana.org/dnssec/ceremonies/51">https://www.iana.org/dnssec/ceremonies/51</a></p>		

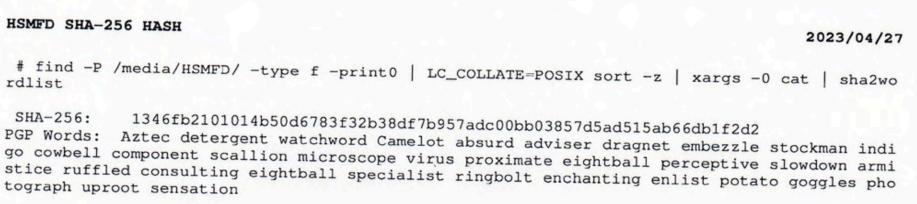
## Printer Setup

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

## Date Setup

Step	Activity	Initials	Time
8	<p>CA executes <code>date</code> using the terminal window to verify if the date/time reasonably matches the ceremony clock.</p> <p>If the date/time do not match, perform the following steps:</p> <ul style="list-style-type: none"> <li>a) Execute <code>date -s "20231130 HH:MM:00"</code> to set the time. where <code>HH</code> is two-digit hour, <code>MM</code> is two-digit minutes and <code>00</code> is zero seconds.</li> <li>b) Execute <code>date</code> to confirm the date/time matches the clock.</li> </ul>		

## Connect the HSMFD

Step	Activity	Initials	Time
9	CA plugs the <b>Ceremony 49 HSMFD</b> into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window.		
10	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD:  <code>hsmfd-hash -c</code>  CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script.    IW confirms that the result matches the SHA-256 hash of the HSMFD using the printed HSMFD hash from the Ceremony 49 OS Media bundle.		

## Distribute Previous HSMFD

Step	Activity	Initials	Time
11	CA gives the unused <b>HSMFD 49</b> and the sheet of paper with the printed HSMFD hash to RKOS.		

## Start the Terminal Session Logging

Step	Activity	Initials	Time
12	CA executes the command below using the terminal window to change the working directory to HSMFD: <code>cd /media/HSMFD</code>		
13	CA executes the command below to log activities of the <b>Commands</b> terminal window: <code>script script-20231130.log</code>		

## Start the HSM Output Logging

Step	Activity	Initials	Time
14	CA performs the following steps using the <b>HSM Output</b> terminal window to capture the activity logs of the HSM: a) Change the working directory to HSMFD by executing: <code>cd /media/HSMFD</code> b) Set the serial port baud rate by executing: <code>stty -F /dev/ttyUSB0 115200</code> c) Start logging the serial output by executing: <code>ttysnoop /dev/ttyUSB0</code>  Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.		

## Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
15	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none"> <li>a) Verify the label on the HSM reads <b>HSM5E</b>.</li> <li>b) Plug the null modem cable into the serial port of the HSM.</li> <li>c) Connect the power to the HSM, then switch it ON.</li> </ul> <p><b>Note: Status information should appear in the HSM output logging screen.</b></p> <ul style="list-style-type: none"> <li>d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads <b>H1903018</b>.</li> <li>e) Scroll down to the end of the logging screen.</li> </ul> <p><b>HSM5E: Serial # H1903018</b></p> <p><b>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</b></p>		

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

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

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

## Crypto Officer Credentials Verification

Step	Activity	Initials	Time
1	<p>The CA calls each of the COs listed below sequentially to perform the following steps:</p> <ul style="list-style-type: none"> <li>a) CO reads aloud the TEB number, then CA inspects it for tamper evidence while IW verifies the information using the previous ceremony script where it was last used.</li> <li>b) CO and CA open the TEB, then the CA removes the plastic case containing the cards as specified below.</li> </ul> <p><b>CO1: Frederico Neves</b>  <b>Set # 1 TEB # BB02639501</b> (Place the cards on the designated card holder)                      Last Verified: KSK Ceremony 47 2022-11-03</p> <p><b>CO2: Pia Gruvö</b>  <b>Set # 1 TEB # BB02639500</b> (Place the cards on the designated card holder)                      Last Verified: KSK Ceremony 47 2022-11-03</p> <p><b>CO4: Robert Seastrom</b>  <b>OP TEB # BB91951237</b> (Place the plastic case on the table for destruction)  <b>SO TEB # BB02639553</b> (Place the plastic case on the table for destruction)  <b>Set # 1 TEB # BB02639552</b> (Place the cards on the designated card holder)                      Last Verified: KSK Ceremony 45 2022-05-12</p> <p><b>CO5: Nomsa Mwayenga</b>  <b>Set # 1 TEB # BB02639496</b> (Place the cards on the designated card holder)                      Last Verified: KSK Ceremony 47 2022-11-03  <b>Set # 2 TEB # BB02639548</b> (Place the plastic case on the table for TEB change)                      Last Verified: KSK Ceremony 45 2022-05-12</p> <p><b>CO6: Hugo Salgado</b>  <b>Set # 1 TEB # BB02638531</b> (Place the cards on the designated card holder)                      Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</b></p>		

## Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
2	<p>CA performs the following steps to activate the HSM:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select "<b>1.Set Online</b>", press <b>ENT</b> to confirm.</li> <li>c) When "<b>Set Online?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>d) When "<b>Insert Card OP #X?</b>" is displayed, insert the OP card.</li> <li>e) When "<b>PIN?</b>" is displayed, enter "<b>11223344</b>", then press <b>ENT</b>.</li> <li>f) When "<b>Remove Card?</b>" is displayed, remove the OP card.</li> <li>g) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> OP cards.</li> </ul> <p>Confirm the "<b>READY</b>" LED on the <b>HSM</b> is <b>ON</b>.                      IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1                      1<sup>st</sup> OP card ____ of 7                      2<sup>nd</sup> OP card ____ of 7                      3<sup>rd</sup> OP card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Check the Network Connectivity Between Laptop and HSM

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

## Insert the KSRFD

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

## Execute the KSR Signer for KSR 2024 Q1

Step	Activity	Initials	Time
6	<p>CA executes the command below in the terminal window to change directory:  <code>cd /media/KSRFD/KSK51/</code></p>		
7	<p>CA executes the command below in the terminal window to sign the KSR file:  <code>kskm-ksrsigner</code></p>		

## Verify the KSR Hash for KSR 2024 Q1

Step	Activity	Initials	Time
8	<p>When the hash of the KSR is displayed in the terminal window, perform the following:</p> <p>a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification <b>off camera</b> for the purpose of authentication while maintaining privacy.</p> <p><b>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></p> <p>b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line:</p> <p><b>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.</b></p> <p>_____</p> <p>c) The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.</p>		
9	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks <b>"are there any objections?"</b>		
10	CA enters <b>Yes</b> in response to <b>"Sign KSR?"</b> to complete the KSR signing operation. The SKR is located in: <code>/media/KSREFD/KSK51/skr-root-2024-q1-0.xml</code>		

## Print Copies of the KSR Signer Log

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



## Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
13	<p>CA deactivates the HSM by performing the following steps:  <b>Note:</b> CA will use OP cards not previously utilized in this ceremony if available.</p> <ol style="list-style-type: none"> <li>CA selects the <b>HSM Output</b> terminal window.</li> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select "<b>2.Set Offline</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Set Offline?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>When "<b>Insert Card OP #X?</b>" is displayed, insert the OP card from the card holder.</li> <li>When "<b>PIN?</b>" is displayed, enter "<b>11223344</b>", then press <b>ENT</b>.</li> <li>When "<b>Remove Card?</b>" is displayed, remove the OP card.</li> <li>Repeat steps e) to g) for the 2<sup>nd</sup> and 3<sup>rd</sup> OP cards.</li> </ol> <p>Confirm the "<b>READY</b>" LED on the <b>HSM</b> is <b>OFF</b>.                      IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1                      1<sup>st</sup> OP card ____ of 7                      2<sup>nd</sup> OP card ____ of 7                      3<sup>rd</sup> OP card ____ of 7</p> <p><b>Note:</b> If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</p>		

## OS Media Checksum Verification

Step	Activity	Initials	Time
14	<p>CA uses the terminal window to executes the following steps:</p> <ol style="list-style-type: none"> <li>Verify the byte count of the SD card matches the ISO size of by running the following command:  <code>df -B1 /dev/sda</code></li> <li>Calculate the SHA-256 hash by executing:  <code>head -c 375431168 /dev/sda   sha2wordlist</code></li> <li>IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.</li> </ol> <p><b>Note:</b> CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.</p> <p>SHA-256 hash:                      405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a</p> <p>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</p> <p><b>Note 1:</b> 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.  <b>Note 2:</b> The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website <a href="https://www.iana.org/dnssec/ceremonies/51">https://www.iana.org/dnssec/ceremonies/51</a></p>		

## Act 4: Destroy OP and SO Cards

The Operator (OP) and Security Officer (SO) cards were originally issued in 2010 and have reached the end of their operational period. New OP and SO card sets were previously generated as replacements, and the original cards will now be destroyed.

The CA will destroy the OP and SO cards by performing the steps below:

- Clear the cards using an HSM's designated clear card function
- Slice through the cards' chips then place the cards in the shredder

### Clear and Destroy OP and SO Cards

Step	Activity	Initials	Time
1	<p>CA performs the following steps to clear Operator (OP) and Security Officer (SO) cards:</p> <ol style="list-style-type: none"> <li>CA selects the <b>HSM Output</b> terminal window.</li> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select <b>"7.Role Mgmt"</b>, press <b>ENT</b> to confirm.</li> <li>When <b>"Insert Card SO #X?"</b> is displayed, insert the SO card.</li> <li>When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>When <b>"Remove Card?"</b> is displayed, remove the SO card.</li> <li>Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SO card.</li> <li>Select <b>"4.Clear RoleCard"</b>, press <b>ENT</b> to confirm.</li> <li>When <b>"Clear Card?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>When <b>"Num Cards?"</b> is displayed, enter <b>"3"</b>, then press <b>ENT</b>.</li> <li>When <b>"Insert Card #X?"</b> is displayed, take the required card, show the card to the audit camera and then insert the card into the HSM's card reader.</li> <li>When <b>"Are you sure?"</b> is displayed, press <b>ENT</b> to confirm.</li> </ol> <p><b>Note: The message will differ depending of the card type.</b></p> <ol style="list-style-type: none"> <li>When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>When <b>"Remove Card?"</b> is displayed, remove the card.</li> <li>Repeat steps k) to n) until the specified cards have been cleared.</li> <li>Press <b>CLR</b> to return to the main menu <b>"Secured"</b>.</li> </ol> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1            1<sup>st</sup> SO card ____ of 7            2<sup>nd</sup> SO card ____ of 7            3<sup>rd</sup> SO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		
2	<p>CA uses the shredder to destroy the cleared OP and SO cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.</p>		

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

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

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

## Issue Temporary Adapter Authorization Key (AAK) Cards

Step	Activity	Initials	Time
1	<p>CA performs the following steps to issue temporary Adapter Authorization Key (AAK) cards:</p> <ul style="list-style-type: none"> <li>a) CA selects the <b>HSM Output</b> terminal window.</li> <li>b) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>c) Select <b>"7.Role Mgmt"</b>, press <b>ENT</b> to confirm.</li> <li>d) When <b>"Insert Card SO #X?"</b> is displayed, insert the SO card.</li> <li>e) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>f) When <b>"Remove Card?"</b> is displayed, remove the SO card.</li> <li>g) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SO card.</li> <li>h) Select <b>"3.Backup AAK"</b>, press <b>ENT</b> to confirm.</li> <li>i) When <b>"Backup AAK?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>j) When <b>"Num Cards?"</b> is displayed, enter <b>"2"</b>, then press <b>ENT</b>.</li> <li>k) When <b>"Insert Card #X?"</b> is displayed, insert the required AAK card.</li> <li>l) When <b>"Remove Card?"</b> is displayed, remove the AAK card.</li> <li>m) Repeat steps k) to l) for the 2<sup>nd</sup> AAK card.</li> <li>n) When <b>"Done AAK"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>o) Press <b>CLR</b> to return to the menu <b>"Secured"</b>.</li> </ul> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> SO card ____ of 7</p> <p>2<sup>nd</sup> SO card ____ of 7</p> <p>3<sup>rd</sup> SO card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</p>		

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

Step	Activity	Initials	Time
2	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections. Note: DO NOT unplug the cable connections on the laptop.		
3	CA places the HSM into its designated new TEB, then seals it.		
4	CA performs the following steps: <ul style="list-style-type: none"> <li>a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.</li> <li>b) Confirm with IW that the TEB number and HSM serial number match below.</li> <li>c) Initial the TEB along with IW using a ballpoint pen.</li> <li>d) Give IW the sealing strips for post-ceremony inventory.</li> <li>e) Place the HSM TEB on the cart.</li> </ul> HSM5E: TEB # BB51184250 / Serial # H1903018		

## Act 6: Introduce New HSM

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

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

### HSM7E (Tier 7) Setup

Step	Activity	Initials	Time
1	<p>CA performs the following steps to prepare the HSM:</p> <ol style="list-style-type: none"> <li>a) Remove the TEB from the cart and place it on the ceremony table.</li> <li>b) Inspect the TEB for tamper evidence.</li> <li>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.</li> <li>d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.</li> </ol> <p><b>HSM7E: TEB # BB51184253 / Serial # H2110009</b>                      Last Verified: AT Ceremony 51 2023-11-29</p> <p><b>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</b></p>		

### Power ON the HSM7E (Tier 7)

Step	Activity	Initials	Time
2	CA selects the <b>HSM Output</b> terminal window.		
3	<p>CA performs the following steps to prepare the HSM:</p> <ol style="list-style-type: none"> <li>a) Verify the label on the HSM reads <b>HSM7E</b>.</li> <li>b) Plug the null modem cable into the serial port of the HSM.</li> <li>c) Connect the power to the HSM, then switch it ON.                              Note: Status information should appear in the HSM output logging screen.</li> <li>d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads <b>H2110009</b>.</li> <li>e) Scroll down to the end of the logging screen.</li> <li>f) After the completion of the HSM self test the display should say <b>"Important Read Manual"</b> indicating the HSM is in the initialized state.</li> </ol> <p><b>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</b></p>		

## Import the AAK

Step	Activity	Initials	Time
4	<p>CA performs the following steps to import the Adapter Authorization Key (AAK):</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select "<b>2.Restore AAK</b>", press <b>ENT</b> to confirm.</li> <li>c) When "<b>Restore AAK?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>d) When "<b>Insert Card #X?</b>" is displayed, insert the required AAK card and press <b>ENT</b>.</li> <li>e) When "<b>Remove Card?</b>" is displayed, remove the AAK card.</li> <li>f) Repeat steps d) to e) for the 2<sup>nd</sup> AAK card.</li> <li>g) When "<b>Done AAK Imported</b>" is displayed, press <b>ENT</b> to confirm.</li> </ul> <p>Each card is returned to its designated card holder after use.</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Configure the HSM to Secure State

Step	Activity	Initials	Time
5	<p>CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select <b>"3.Secure"</b>, press <b>ENT</b> to confirm.</li> <li>c) When <b>"Secure?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>d) When <b>"Insert Card SO #X?"</b> is displayed, insert the SO card.</li> <li>e) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>f) When <b>"Remove Card?"</b> is displayed, remove the SO card.</li> <li>g) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SO cards.</li> <li>h) When <b>"SMK AES Triple DES?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>i) When <b>"SMK AES"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>j) When <b>"LAN Port Number?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>k) When <b>"Enable IPv4/IPv6?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>l) When <b>"LAN IPv4 Address?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>m) When <b>"LAN IPv4 Mask?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>n) When <b>"Set IPv4 Gateway?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>o) When <b>"LAN IPv6 Address?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>p) When <b>"LAN IPv6 Mask?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>q) When <b>"Set IPv6 Gateway?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>r) When <b>"Remote Mgmt Off Enable?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>s) When <b>"Remote Mgmt Off"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>t) When <b>"Change Clock?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>u) When <b>"Import Config?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>v) When <b>"FIPS Mode On Disable?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>w) When <b>"FIPS Mode On"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>x) When <b>"Global Key Export Enabled"</b> is displayed, press <b>CLR</b> to skip.</li> </ul> <p><b>Done Rebooting Device</b> will be displayed.                      IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1                      1<sup>st</sup> SO card ____ of 7                      2<sup>nd</sup> SO card ____ of 7                      3<sup>rd</sup> SO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Change the API Settings

Step	Activity	Initials	Time
6	<p>CA performs the following steps to change the API settings:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select "<b>5.Key Mgmt</b>", press <b>ENT</b> to confirm.</li> <li>c) When "<b>Insert CO Card #X?</b>" is displayed, insert the CO card.</li> <li>d) When "<b>PIN?</b>" is displayed, enter "<b>11223344</b>", then press <b>ENT</b>.</li> <li>e) When "<b>Remove Card?</b>" is displayed, remove the CO card.</li> <li>f) Repeat steps c) to e) for the 2<sup>nd</sup> and 3<sup>rd</sup> CO card.</li> <li>g) Select "<b>5. API Settings</b>", press <b>ENT</b> to confirm.</li> <li>h) Select "<b>1.Key Import</b>", press <b>ENT</b> to confirm.</li> <li>i) When "<b>Key Import On Disable?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>j) Select "<b>2.Key Export</b>", press <b>ENT</b> to confirm.</li> <li>k) When "<b>Key Export On Disable?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>l) Select "<b>5.Sym Key Der</b>", press <b>ENT</b> to confirm.</li> <li>m) When "<b>Sym Key Der On Disable?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>n) Press <b>CLR twice</b> to return to the main menu "<b>Secured</b>".</li> </ul> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> CO card ____ of 7</p> <p>2<sup>nd</sup> CO card ____ of 7</p> <p>3<sup>rd</sup> CO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		



## Verify API Settings

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

## App Key Backups

Step	Activity	Initials	Time
8	<p>CA performs the following steps to prepare the App key backups:</p> <ol style="list-style-type: none"> <li>Remove the TEB from the cart and place it on the ceremony table.</li> <li>Inspect the TEB for tamper evidence.</li> <li>Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used.</li> <li>Remove and discard the TEB, then place the App key cards and the backup HSMFD on its designated area of the ceremony table.</li> <li>If not already present, place corresponding labels on the APP key plastic case and ensure their respective HSMFDs remain in the plastic case.</li> </ol> <p><b>KSK-2017: TEB # BB46584614</b>  Last Verified: KSK Ceremony 43 2021-10-14  <b>KSK-2023: TEB # BB02638526</b>  Last Verified: KSK Ceremony 49 2023-04-27</p> <p><b>Note:</b> "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</p>		

## Import the SMK and the KSK

Step	Activity	Initials	Time
9	<p>CA performs the following steps to access the Key Management menu:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select <b>"5.Key Mgmt"</b>, press <b>ENT</b> to confirm.</li> <li>c) When <b>"Insert CO Card #X?"</b> is displayed, insert the CO card.</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>e) When <b>"Remove Card?"</b> is displayed, remove the CO card.</li> <li>f) Repeat steps c) to e) for the 2<sup>nd</sup> and 3<sup>rd</sup> CO card.</li> </ul> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> CO card ____ of 7</p> <p>2<sup>nd</sup> CO card ____ of 7</p> <p>3<sup>rd</sup> CO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

Step	Activity	Initials	Time
10	<p>CA performs the following steps to import the SMK:</p> <ol style="list-style-type: none"> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select "<b>4.SMK</b>" from the current "<b>Key Mgmt</b>" menu, press <b>ENT</b> to confirm.</li> <li>Select "<b>3.Restore SMK</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Restore SMK?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>When "<b>Insert Card SMK #X?</b>" is displayed, insert the SMK card.</li> <li>When "<b>Remove Card?</b>" is displayed, remove the SMK card.</li> <li>Repeat steps e) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SMK card.</li> <li>When "<b>SMK Restored</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>Press <b>CLR</b> once to return to the menu "<b>Key Mgmt</b>".</li> </ol> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> SMK card ____ of 7</p> <p>2<sup>nd</sup> SMK card ____ of 7</p> <p>3<sup>rd</sup> SMK card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		
11	<p>CA performs the following steps to import KSK:</p> <ol style="list-style-type: none"> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select "<b>3.App Keys</b>" from the current "<b>Key Mgmt</b>" menu, press <b>ENT</b> to confirm.</li> <li>Select "<b>2.Restore</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Restore?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>When "<b>Which Media?</b>" is displayed, select "<b>2. From Card</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Insert Card #X?</b>" is displayed, insert the required KSK card.</li> <li>When "<b>Remove Card?</b>" is displayed, remove the KSK card.</li> <li>When "<b>Restore Complete</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>Repeat steps c) to h) for any remaining App Key card listed below.</li> <li>Press <b>CLR twice</b> to return to the main menu "<b>Secured</b>".</li> </ol> <p>CA uses the card listed below. Card is returned to its designated card holder after use.</p> <p><b>KSK-2017: Klajeyz App Key card # 1</b></p> <p><b>KSK-2023: Kmrfl3b App Key card # 1</b></p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
12	<p>CA performs the following steps to activate the HSM:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select "<b>1.Set Online</b>", press <b>ENT</b> to confirm.</li> <li>c) When "<b>Set Online?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>d) When "<b>Insert Card OP #X?</b>" is displayed, insert the OP card.</li> <li>e) When "<b>PIN?</b>" is displayed, enter "<b>11223344</b>", then press <b>ENT</b>.</li> <li>f) When "<b>Remove Card?</b>" is displayed, remove the OP card.</li> <li>g) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> OP cards.</li> </ul> <p>Confirm the "<b>READY</b>" LED on the <b>HSM</b> is <b>ON</b>.                      IW records which cards were used below. Each card is returned to its designated card holder after use.                      Set # 1                      1<sup>st</sup> OP card ____ of 7                      2<sup>nd</sup> OP card ____ of 7                      3<sup>rd</sup> OP card ____ of 7</p> <p><b>Note:</b> If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</p>		

## Check the Network Connectivity Between Laptop and HSM

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

## Execute the KSR Signer for KSR 2024 Q1

Step	Activity	Initials	Time
15	CA executes the command below in the terminal window to change directory: <code>cd HSM7E/</code>		
16	CA executes the command below in the terminal window to sign the KSR file: <code>kskm-ksrsigner</code>		

## Verify the KSR Hash for KSR 2024 Q1

Step	Activity	Initials	Time
17	The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.		
18	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks "are there any objections?"		
19	CA enters <b>Yes</b> in response to "Sign KSR?" to complete the KSR signing operation. The SKR is located in: /media/KSRFD/KSK51/HSM7E/HSM7E-skr-root-2024-q1-0.xml		

## Print Copies of the KSR Signer log

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

## SKR Comparison

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

## Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
25	<p>CA deactivates the HSM by performing the following steps:  <b>Note: CA will use OP cards not previously utilized in this ceremony if available.</b></p> <ol style="list-style-type: none"> <li>CA selects the <b>HSM Output</b> terminal window.</li> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select <b>"2.Set Offline"</b>, press <b>ENT</b> to confirm.</li> <li>When <b>"Set Offline?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>When <b>"Insert Card OP #X?"</b> is displayed, insert the OP card from the card holder.</li> <li>When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>When <b>"Remove Card?"</b> is displayed, remove the OP card.</li> <li>Repeat steps e) to g) for the 2<sup>nd</sup> and 3<sup>rd</sup> OP cards.</li> </ol> <p>Confirm the <b>"READY"</b> LED on the <b>HSM</b> is <b>OFF</b>.                      IW records which cards were used below. Each card is returned to its designated card holder after use.                      Set # 1                      1<sup>st</sup> OP card ____ of 7                      2<sup>nd</sup> OP card ____ of 7                      3<sup>rd</sup> OP card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

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

Step	Activity	Initials	Time
26	<p>CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.  <b>Note: DO NOT unplug the cable connections on the laptop.</b></p>		
27	<p>CA places the HSM into its designated new TEB, then seals it.</p>		
28	<p>CA performs the following steps:</p> <ol style="list-style-type: none"> <li>Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.</li> <li>Confirm with IW that the TEB number and HSM serial number match below.</li> <li>Initial the TEB along with IW using a ballpoint pen.</li> <li>Give IW the sealing strips for post-ceremony inventory.</li> <li>Place the HSM TEB on the cart.</li> </ol> <p><b>HSM7E: TEB # BB51184251 / Serial # H2110009</b></p>		

## HSM8E (Tier 7) Setup

Step	Activity	Initials	Time
29	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none"> <li>a) Remove the TEB from the cart and place it on the ceremony table.</li> <li>b) Inspect the TEB for tamper evidence.</li> <li>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.</li> <li>d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table.</li> </ul> <p><b>HSM8E: TEB # BB51184254 / Serial # H2110010</b>                      Last Verified: AT Ceremony 51 2023-11-29</p> <p><b>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</b></p>		

## Power ON the HSM8E (Tier 7)

Step	Activity	Initials	Time
30	CA selects the <b>HSM Output</b> terminal window.		
31	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none"> <li>a) Verify the label on the HSM reads <b>HSM8E</b>.</li> <li>b) Plug the null modem cable into the serial port of the HSM.</li> <li>c) Connect the power to the HSM, then switch it ON.</li> </ul> <p><b>Note: Status information should appear in the HSM output logging screen.</b></p> <ul style="list-style-type: none"> <li>d) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads <b>H2110010</b>.</li> <li>e) Scroll down to the end of the logging screen.</li> <li>f) After the completion of the HSM self test the display should say <b>"Important Read Manual"</b> indicating the HSM is in the initialized state.</li> </ul> <p><b>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</b></p>		

## Import the AAK

Step	Activity	Initials	Time
32	<p>CA performs the following steps to import the Adapter Authorization Key (AAK):</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select <b>"2.Restore AAK"</b>, press <b>ENT</b> to confirm.</li> <li>c) When <b>"Restore AAK?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>d) When <b>"Insert Card #X?"</b> is displayed, insert the required AAK card and press <b>ENT</b>.</li> <li>e) When <b>"Remove Card?"</b> is displayed, remove the AAK card.</li> <li>f) Repeat steps d) to e) for the 2<sup>nd</sup> AAK card.</li> <li>g) When <b>"Done AAK Imported"</b> is displayed, press <b>ENT</b> to confirm.</li> </ul> <p>Each card is returned to its designated card holder after use.</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Configure the HSM to Secure State

Step	Activity	Initials	Time
33	<p>CA performs the following steps, ensuring that three cards from only one of the two SO card sets are utilized to configure the HSM to secure state:</p> <ol style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select <b>"3.Secure"</b>, press <b>ENT</b> to confirm.</li> <li>c) When <b>"Secure?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>d) When <b>"Insert Card SO #X?"</b> is displayed, insert the SO card.</li> <li>e) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>f) When <b>"Remove Card?"</b> is displayed, remove the SO card.</li> <li>g) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SO cards.</li> <li>h) When <b>"SMK AES Triple DES?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>i) When <b>"SMK AES"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>j) When <b>"LAN Port Number?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>k) When <b>"Enable IPv4/IPv6?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>l) When <b>"LAN IPv4 Address?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>m) When <b>"LAN IPv4 Mask?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>n) When <b>"Set IPv4 Gateway?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>o) When <b>"LAN IPv6 Address?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>p) When <b>"LAN IPv6 Mask?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>q) When <b>"Set IPv6 Gateway?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>r) When <b>"Remote Mgmt Off Enable?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>s) When <b>"Remote Mgmt Off</b> is displayed, press <b>ENT</b> to confirm.</li> <li>t) When <b>"Change Clock?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>u) When <b>"Import Config?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>v) When <b>"FIPS Mode On Disable?"</b> is displayed, press <b>CLR</b> to skip.</li> <li>w) When <b>"FIPS Mode On"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>x) When <b>"Global Key Export Enabled"</b> is displayed, press <b>CLR</b> to skip.</li> </ol> <p><b>Done Rebooting Device</b> will be displayed.                      IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1                      1<sup>st</sup> SO card ____ of 7                      2<sup>nd</sup> SO card ____ of 7                      3<sup>rd</sup> SO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</b></p>		



## Change the API Settings

Step	Activity	Initials	Time
34	<p>CA performs the following steps to change the API settings:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select <b>"5.Key Mgmt"</b>, press <b>ENT</b> to confirm.</li> <li>c) When <b>"Insert CO Card #X?"</b> is displayed, insert the CO card.</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>e) When <b>"Remove Card?"</b> is displayed, remove the CO card.</li> <li>f) Repeat steps c) to e) for the 2<sup>nd</sup> and 3<sup>rd</sup> CO card.</li> <li>g) Select <b>"5. API Settings"</b>, press <b>ENT</b> to confirm.</li> <li>h) Select <b>"1.Key Import"</b>, press <b>ENT</b> to confirm.</li> <li>i) When <b>"Key Import On Disable?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>j) Select <b>"2.Key Export"</b>, press <b>ENT</b> to confirm.</li> <li>k) When <b>"Key Export On Disable?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>l) Select <b>"5.Sym Key Der"</b>, press <b>ENT</b> to confirm.</li> <li>m) When <b>"Sym Key Der On Disable?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>n) Press <b>CLR twice</b> to return to the main menu <b>"Secured"</b>.</li> </ul> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> CO card ____ of 7</p> <p>2<sup>nd</sup> CO card ____ of 7</p> <p>3<sup>rd</sup> CO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Verify API Settings

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

## Import the SMK and the KSK

Step	Activity	Initials	Time
36	<p>CA performs the following steps to access the Key Management menu:</p> <ol style="list-style-type: none"> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select <b>"5.Key Mgmt"</b>, press <b>ENT</b> to confirm.</li> <li>When <b>"Insert CO Card #X?"</b> is displayed, insert the CO card.</li> <li>When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>When <b>"Remove Card?"</b> is displayed, remove the CO card.</li> <li>Repeat steps c) to e) for the 2<sup>nd</sup> and 3<sup>rd</sup> CO card.</li> </ol> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <pre> Set # 1 1<sup>st</sup> CO card ____ of 7 2<sup>nd</sup> CO card ____ of 7 3<sup>rd</sup> CO card ____ of 7                     </pre> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

Step	Activity	Initials	Time
37	<p>CA performs the following steps to import the SMK:</p> <ol style="list-style-type: none"> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select "<b>4.SMK</b>" from the current "<b>Key Mgmt</b>" menu, press <b>ENT</b> to confirm.</li> <li>Select "<b>3.Restore SMK</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Restore SMK?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>When "<b>Insert Card SMK #X?</b>" is displayed, insert the SMK card.</li> <li>When "<b>Remove Card?</b>" is displayed, remove the SMK card.</li> <li>Repeat steps e) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SMK card.</li> <li>When "<b>SMK Restored</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>Press <b>CLR</b> once to return to the menu "<b>Key Mgmt</b>".</li> </ol> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> SMK card ____ of 7</p> <p>2<sup>nd</sup> SMK card ____ of 7</p> <p>3<sup>rd</sup> SMK card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		
38	<p>CA performs the following steps to import KSK:</p> <ol style="list-style-type: none"> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select "<b>3.App Keys</b>" from the current "<b>Key Mgmt</b>" menu, press <b>ENT</b> to confirm.</li> <li>Select "<b>2.Restore</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Restore?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>When "<b>Which Media?</b>" is displayed, select "<b>2. From Card</b>", press <b>ENT</b> to confirm.</li> <li>When "<b>Insert Card #X?</b>" is displayed, insert the required KSK card.</li> <li>When "<b>Remove Card?</b>" is displayed, remove the KSK card.</li> <li>When "<b>Restore Complete</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>Repeat steps c) to h) for any remaining App Key card listed below.</li> <li>Press <b>CLR twice</b> to return to the main menu "<b>Secured</b>".</li> </ol> <p>CA uses the card listed below. Card is returned to its designated card holder after use.</p> <p><b>KSK-2017: Klajeyz App Key card # 2</b></p> <p><b>KSK-2023: Kmrfl3b App Key card # 2</b></p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
39	<p>CA performs the following steps to activate the HSM:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select "<b>1.Set Online</b>", press <b>ENT</b> to confirm.</li> <li>c) When "<b>Set Online?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>d) When "<b>Insert Card OP #X?</b>" is displayed, insert the OP card.</li> <li>e) When "<b>PIN?</b>" is displayed, enter "<b>11223344</b>", then press <b>ENT</b>.</li> <li>f) When "<b>Remove Card?</b>" is displayed, remove the OP card.</li> <li>g) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> OP cards.</li> </ul> <p>Confirm the "<b>READY</b>" LED on the <b>HSM</b> is <b>ON</b>.                      IW records which cards were used below. Each card is returned to its designated card holder after use.                      Set # 1                      1<sup>st</sup> OP card ____ of 7                      2<sup>nd</sup> OP card ____ of 7                      3<sup>rd</sup> OP card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again.                      For a summary of card roles and their purpose see Appendix A number [14].</b></p>		

## Check the Network Connectivity Between Laptop and HSM

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

## Execute the KSR Signer for KSR 2024 Q1

Step	Activity	Initials	Time
42	CA executes the command below in the terminal window to change directory: <code>cd HSM8E/</code>		
43	CA executes the command below in the terminal window to sign the KSR file: <code>kskm-ksrsigner</code>		

## Verify the KSR Hash for KSR 2024 Q1

Step	Activity	Initials	Time
44	The CA asks some participants to compare the hash in the email sent by the RZM representative prior to the ceremony and some participants to compare the hash in the terminal window, then asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file being used.		
45	Participants confirm that the hash matches with the RZM representative's discourse, then CA asks "are there any objections?"		
46	CA enters <b>Yes</b> in response to "Sign KSR?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSRFD/KSK51/HSM8E/HSM8E-skr-root-2024-q1-0.xml</code>		

## Print Copies of the KSR Signer log

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

## SKR Comparison

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

## Copy the Newly Generated SKR

Step	Activity	Initials	Time
52	<p>CA executes the following commands using the terminal window:</p> <ul style="list-style-type: none"> <li>a) List the contents of the KSRFD by executing: <code>ls -ltrR /media/KSRFD</code></li> <li>b) Copy the contents of the KSRFD to the HSMFD by executing: <code>cp -pR /media/KSRFD/* .</code></li> </ul> <p>Note: Confirm overwrite by entering "y" if prompted.</p> <ul style="list-style-type: none"> <li>c) List the contents of the HSMFD by executing: <code>ls -ltrR</code></li> <li>d) Verify it has been copied successfully by executing: <code>diff -qr /media/HSMFD/KSK51/ /media/KSRFD/KSK51/</code></li> <li>e) Unmount the KSRFD by executing: <code>umount /media/KSRFD</code></li> </ul>		
53	<p>CA removes the <b>KSRFD</b> containing the SKR files, then gives it to the RZM representative.</p> <p>Note: If the RZM representative is participating remotely, RKOS will take custody of the KSRFD instead.</p>		

## Disable/Deactivate the HSM (Tier 7)

Step	Activity	Initials	Time
54	<p>CA deactivates the HSM by performing the following steps:</p> <p>Note: CA will use OP cards not previously utilized in this ceremony if available.</p> <ul style="list-style-type: none"> <li>a) CA selects the <b>HSM Output</b> terminal window.</li> <li>b) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>c) Select "<b>2.Set Offline</b>", press <b>ENT</b> to confirm.</li> <li>d) When "<b>Set Offline?</b>" is displayed, press <b>ENT</b> to confirm.</li> <li>e) When "<b>Insert Card OP #X?</b>" is displayed, insert the OP card from the card holder.</li> <li>f) When "<b>PIN?</b>" is displayed, enter "<b>11223344</b>", then press <b>ENT</b>.</li> <li>g) When "<b>Remove Card?</b>" is displayed, remove the OP card.</li> <li>h) Repeat steps e) to g) for the 2<sup>nd</sup> and 3<sup>rd</sup> OP cards.</li> </ul> <p>Confirm the "<b>READY</b>" LED on the <b>HSM</b> is <b>OFF</b>. IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1</p> <p>1<sup>st</sup> OP card ____ of 7 2<sup>nd</sup> OP card ____ of 7 3<sup>rd</sup> OP card ____ of 7</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</p>		

## Clear and Destroy AAK Cards

Step	Activity	Initials	Time
55	<p>CA performs the following steps to clear Adapter Authorization Key (AAK) cards:</p> <ul style="list-style-type: none"> <li>a) Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>b) Select <b>"7.Role Mgmt"</b>, press <b>ENT</b> to confirm.</li> <li>c) When <b>"Insert Card SO #X?"</b> is displayed, insert the SO card.</li> <li>d) When <b>"PIN?"</b> is displayed, enter <b>"11223344"</b>, then press <b>ENT</b>.</li> <li>e) When <b>"Remove Card?"</b> is displayed, remove the SO card.</li> <li>f) Repeat steps d) to f) for the 2<sup>nd</sup> and 3<sup>rd</sup> SO card.</li> <li>g) Select <b>"5.Clear AAK Card"</b>, press <b>ENT</b> to confirm.</li> <li>h) When <b>"Clear AAK Card?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>i) When <b>"Num Cards?"</b> is displayed, enter <b>"2"</b>, then press <b>ENT</b>.</li> <li>j) When <b>"Insert Card AAK #X?"</b> is displayed, take the <b>AAK #X</b> card from the cardholder, show the <b>AAK #X</b> card to the audit camera and then insert the <b>AAK #X</b> card into the HSM's card reader.</li> <li>k) When <b>"Are you sure?"</b> is displayed, press <b>ENT</b> to confirm.</li> <li>l) When <b>"Remove Card?"</b> is displayed, remove the AAK card.</li> <li>m) Repeat steps j) to l) for the 2<sup>nd</sup> AAK card.</li> <li>n) Press <b>CLR</b> to return to the main menu <b>"Secured"</b>.</li> </ul> <p>IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>Set # 1                      1<sup>st</sup> SO card ____ of 7                      2<sup>nd</sup> SO card ____ of 7                      3<sup>rd</sup> SO card ____ of 7</p> <p><b>Note: If a card is unreadable, gently wipe its metal contacts and try again. For a summary of card roles and their purpose see Appendix A number [14].</b></p>		
56	<p>CA uses the shredder to destroy the cleared AAK cards. Use scissors to slice through the center of the chip before inserting cards into the shredder.</p>		

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

Step	Activity	Initials	Time
57	<p>CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.</p> <p><b>Note: DO NOT unplug the cable connections on the laptop.</b></p>		
58	<p>CA places the HSM into its designated new TEB, then seals it.</p>		
59	<p>CA performs the following steps:</p> <ul style="list-style-type: none"> <li>a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.</li> <li>b) Confirm with IW that the TEB number and HSM serial number match below.</li> <li>c) Initial the TEB along with IW using a ballpoint pen.</li> <li>d) Give IW the sealing strips for post-ceremony inventory.</li> <li>e) Place the HSM TEB on the cart.</li> </ul> <p><b>HSM8E: TEB # BB51184252 / Serial # H2110010</b></p>		

## Return the KSK into a TEB

Step	Activity	Initials	Time
60	CA places the KSK and the backup HSMFD into its designated new TEB, then seals it.		
61	<p>CA performs the following steps:</p> <ul style="list-style-type: none"> <li>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.</li> <li>b) Confirm with IW that the TEB number matches below.</li> <li>c) Initial the TEB along with IW using a ballpoint pen.</li> <li>d) Give IW the sealing strips for post-ceremony inventory.</li> <li>e) Place the KSK TEB on the cart.</li> </ul> <p><b>KSK-2017: TEB # BB02638662</b>  <b>KSK-2023: TEB # BB02638661</b></p>		



# Act 7: Secure Hardware

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

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

## Stop Logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
1	CA performs the following steps to stop logging: <ol style="list-style-type: none"> <li>a) Perform the following steps using the <b>HSM Output</b> terminal window to stop logging the serial output (<b>ttyaudit</b>):                             <ol style="list-style-type: none"> <li>i) Press <b>Ctrl + C</b></li> <li>ii) Execute <b>exit</b></li> </ol> </li> <li>b) Execute the command below using the <b>Commands</b> terminal window to stop logging the terminal session: <b>exit</b></li> </ol> <p><b>Note:</b> The <b>Commands</b> terminal session window will remain open.</p> <ol style="list-style-type: none"> <li>c) Disconnect the null modem and ethernet cables from the laptop.</li> </ol>		

## Print Logging Information

Step	Activity	Initials	Time
2	CA executes the following commands to print a copy of the logging information: <ol style="list-style-type: none"> <li>a) <code>print-script script-202311*.log</code></li> <li>b) <code>print-ttyaudit ttyaudit-tty*-202311*.log</code></li> </ol> <p>Attach the printed copies to IW script.</p> <p><b>Note:</b> Ignore the error regarding non-printable characters if prompted.</p>		

## Prepare blank FDs and Copy the HSMFD Contents

Step	Activity	Initials	Time
3	CA executes the following command to print <b>two</b> copies of the hash for the HSMFD content: <pre>hsmfd-hash -p</pre> <p><b>Note:</b> One copy for audit bundle and one copy for HSMFD package.</p>		
4	CA executes the command below to display the contents of the HSMFD: <pre>ls -ltrR</pre>		
5	CA executes the command below to set the <code>copy-hsmfd</code> script to verbose mode: <pre>sed -i '4i set -x' /opt/icann/bin/copy-hsmfd</pre>		
6	CA executes the command below to create <b>five</b> HSMFDs copies: <pre>copy-hsmfd</pre> <p><b>Note:</b> Wait for the activity light on the copy HSMFD to stop flashing before removal.</p>		

## Place HSMFDs and OS Media into a TEB

Step	Activity	Initials	Time
7	<p>CA executes the following commands using the terminal window to unmount the HSMFD:</p> <ul style="list-style-type: none"> <li>a) <code>cd /tmp</code></li> <li>b) <code>umount /media/HSMFD</code></li> </ul> <p>CA removes the HSMFD, then places it on the holder.  <b>Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.</b></p>		
8	<p>CA performs the following steps to switch OFF the laptop and remove the OS media:</p> <ul style="list-style-type: none"> <li>a) Turn OFF the laptop by pressing the power button.</li> <li>b) Disconnect all connections from the laptop.</li> <li>c) Remove the OS media from the laptop.</li> </ul>		
9	<p>CA places 2 HSMFDs, 2 OS media SD cards enclosed in their plastic cases, 2 OS media DVDs, and 1 sheet of paper with the printed HSMFD hash into its designated new TEB, then seals it.</p>		
10	<p>CA performs the following steps to verify the TEB:</p> <ul style="list-style-type: none"> <li>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.</li> <li>b) Confirm with IW that the TEB number matches with the information below.</li> <li>c) Initial the TEB along with IW using a ballpoint pen.</li> <li>d) Give IW the sealing strips for post-ceremony inventory.</li> <li>e) Place the OS media TEB on the cart.</li> </ul> <p><b>OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663</b></p>		
11	<p>CA distributes the following HSMFDs:</p> <ul style="list-style-type: none"> <li>2 for IW (for audit bundles).</li> <li>2 for RKOS (for SKR exchange with RZM and process review).</li> </ul>		

## Place the Laptop into a TEB

Step	Activity	Initials	Time
12	<p>CA places the laptop into its designated new TEB, then seals it.</p>		
13	<p>CA performs the following steps:</p> <ul style="list-style-type: none"> <li>a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see.</li> <li>b) Confirm with IW that the TEB number and laptop serial number matches with the information below.</li> <li>c) Initial the TEB along with IW using a ballpoint pen.</li> <li>d) Give IW the sealing strips for post-ceremony inventory.</li> <li>e) Place the laptop TEB on the cart.</li> </ul> <p><b>Laptop4: TEB # BB81420078 / Service Tag # 58SVSG2</b></p>		

## Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
14	<p>The CA calls each of the COs listed below sequentially to the ceremony table to perform the following steps:</p> <ol style="list-style-type: none"> <li>CA takes the TEB and plastic case prepared for the CO.</li> <li>CO takes their cards from the card holder and places them inside the plastic case.</li> <li>CO gives the plastic case containing the cards to the CA.</li> <li>CA places the plastic case into its designated new TEB, reads aloud the TEB number and description, then seals it.</li> <li>CA initials the TEB with a ballpoint pen, then IW keeps the sealing strips for post-ceremony inventory.</li> <li>IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.</li> <li>CA gives the TEB containing the cards to the CO.</li> <li>CO inspects the TEB, verifies its contents, then initials it with a ballpoint pen.</li> <li>CO writes the date and time, then signs the table of the IW's script, then the IW initials the entry.</li> <li>CO returns to their seat with their TEBs, being especially careful not to compromise any TEB.</li> <li>Repeat steps for all the remaining COs' credentials on the list.</li> </ol> <p><b>CO1: Frederico Neves</b> Set # 1 TEB # BB02638669</p> <p><b>CO2: Pia Gruvö</b> Set # 1 TEB # BB02638668</p> <p><b>CO4: Robert Seastrom</b> Set # 1 TEB # BB02638667</p> <p><b>CO5: Nomsa Mwayenga</b> Set # 1 TEB # BB02638666 Set # 2 TEB # BB02638665 (CO reviews the card set prior to placing into TEB)</p> <p><b>CO6: Hugo Salgado</b> Set # 1 TEB # BB02638664</p>		

<b>CO</b>	<b>TEB #</b>	<b>Printed Name</b>	<b>Signature</b>	<b>Date</b>	<b>Time</b>	<b>IW Initials</b>
<b>CO1</b>	Set # 1 TEB # <b>BB02638669</b>	<b>Frederico Neves</b>		<b>2023 Nov __</b>		
<b>CO2</b>	Set # 1 TEB # <b>BB02638668</b>	<b>Pia Gruvö</b>		<b>2023 Nov __</b>		
<b>CO4</b>	Set # 1 TEB # <b>BB02638667</b>	<b>Robert Seastrom</b>		<b>2023 Nov __</b>		
<b>CO5</b>	Set # 1 TEB # <b>BB02638666</b> Set # 2 TEB # <b>BB02638665</b>	<b>Nomsa Mwayenga</b>		<b>2023 Nov __</b>		
<b>CO6</b>	Set # 1 TEB # <b>BB02638664</b>	<b>Hugo Salgado</b>		<b>2023 Nov __</b>		

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

Step	Activity	Initials	Time
15	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
16	SSC1 opens Safe #1 while shielding the combination from the camera. <b>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.</b>		
17	SSC1 removes the safe log, then writes the date and time, then signs the safe log where <b>"Open Safe"</b> is indicated. IW verifies this entry, then initials it. <b>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</b>		
18	CA performs the following steps to return each piece of equipment to the safe: a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where <b>"Return"</b> is indicated. d) IW verifies the safe log entry, then initials it.  <b>HSM5E: TEB # BB51184250</b> <b>HSM7E: TEB # BB51184251</b> <b>HSM8E: TEB # BB51184252</b> <b>Laptop4: TEB # BB81420078</b> <b>OS media (release coen-1.0.0) + HSMFD: TEB # BB02638663</b> <b>KSK-2017: TEB # BB02638662</b> <b>KSK-2023: TEB # BB02638661</b>		

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

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

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

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

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

Step	Activity	Initials	Time
25	<p>COs perform the following steps sequentially to return the listed TEBs:</p> <ul style="list-style-type: none"> <li>a) CO reads aloud the TEB number(s), then verifies integrity while showing the TEB(s) to the audit camera above</li> <li>b) After the CA operates the guard key in the bottom lock, CO reads aloud the safe deposit box number and uses their tenant key to operate the top lock.</li> </ul> <p><b>Note:</b> The COs will retrieve their new safe deposit box keys when specified below.</p> <ul style="list-style-type: none"> <li>c) CO opens their safe deposit box, places their TEB(s) inside, then closes and locks the safe deposit box.</li> <li>d) CO writes the date and time, then signs the safe log where <b>"Return"</b> is indicated.</li> <li>e) IW verifies the completed safe log entry, then initials it.</li> </ul> <p><b>CO1: Frederico Neves</b>  <b>Box # 1239</b>  <b>Set # 1 TEB # BB02638669</b></p> <p><b>CO2: Pia Gruvö</b>  <b>Box # 1264</b>  <b>Set # 1 TEB # BB02638668</b></p> <p><b>CO4: Robert Seastrom</b>  <b>Box # 1243</b>  <b>Set # 1 TEB # BB02638667</b></p> <p><b>CO5: Nomsa Mwayenga</b>  <b>Box # 1262</b>  <b>Set # 1 TEB # BB02638666</b>  <b>Set # 2 TEB # BB02638665</b></p> <p><b>CO6: Hugo Salgado</b>  <b>Box # 1242</b>  <b>Set # 1 TEB # BB02638664</b></p>		

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

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

# Act 8: Close the Key Signing Ceremony

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

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

## Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.		
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. <b>All signatories declare that this script is a true and accurate record of the ceremony.</b>		
3	CA reviews IW's script, then signs the participants list.		
4	IW signs the list and records the completion time.		

## Stop Online Streaming and Recording

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

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

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

## Bundle Audit Materials

Step	Activity	Initials	Time
10	<p>IW makes a copy of their script for off-site audit bundle containing:</p> <ul style="list-style-type: none"> <li>a) Output of signer system - HSMFD.</li> <li>b) Copy of IW's key ceremony script.</li> <li>c) Audio-visual recording from the audit cameras.</li> <li>d) Logs from the Physical Access Control System and Intrusion Detection System: Range: <b>20230427 00:00:00 to 20231131 00:00:00 UTC</b></li> <li>e) IW's attestation (See Appendix C on page 51).</li> <li>f) SA's attestation (See Appendix D on page 52 and Appendix E on page 53).</li> </ul> <p>All TEBs are labeled <b>Root DNSSEC KSK Ceremony 51</b>, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>		

## Appendix A: Glossary

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

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

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

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

- [4] **hsmfd-hash**:\* A bash script used to calculate, print, and compare SHA-256 checksums for the HSMFD flash drives.

**Note: The sort command has different behavior depending on the locale settings specified by environment variables. Current OS locale setting is LC\_COLLATE="POSIX"**

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

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

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

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

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

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

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

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

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

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

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

---

\* The source code is available at [https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-1.0.0coen\\_amd64.deb](https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-1.0.0coen_amd64.deb)

A debian package is an **ar** archive. To extract data from a deb package, use the command **ar -x ksk-tools-1.0.0coen\_amd64.deb**

Then extract the files with **tar -xvf data.tar.xz**

The file will be located in the directory: **./opt/icann/bin/**

---

\*\* The source code is available at <https://github.com/iana-org/dnssec-keytools>



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

- a) **OP (Operator)**: Configures the HSM to an online or offline state toggling communication through its ethernet adapter. Required for communication with the laptop for key signing operations.
- b) **SO (Security Officer)**: Used for HSM administrative operations. Required to create other role cards (OP and CO), and the introduction or zeroization of an HSM.
- c) **CO (Crypto Officer)**: Used for the key management functions in an HSM. Required for adding or deleting keys stored in an HSM.
- d) **SMK (Storage Master Key)**: Allows an HSM to read an encrypted APP key backup. Required for initial migration of keys and disaster recovery.
- e) **AAK (Adapter Authorization Key)**: Configures an HSM to use previously generated OP, CO, and SO cards. Required for the introduction of an HSM.
- f) **APP (Application Key)**: An encrypted backup copy of one or more keys stored in an HSM, which can only be decoded by its corresponding SMK. Required for migrating keys and disaster recovery.

## **Appendix B: Audit Bundle Checklist**

### **1. Output of Signer System (by CA)**

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

### **2. Key Ceremony Script (by IW)**

Hard copies of the IW's key ceremony script, notes generated during the ceremony, and attestation. See Appendix C on page 51.

### **3. Audio-Visual Recordings from the KSK Ceremony (by SA)**

Two sets of the audit camera footage - One for the original audit bundle and the other for the duplicate audit bundle.

### **4. Logs from the Physical Access Control System and Intrusion Detection System (by SA)**

Two electronic copies of the following:

1. Firewall configuration
2. Configuration reports
3. Personnel/cardholder reports
4. Activity and audit log reports

These files will be placed inside two separate Flash Drives that are labeled "Audit".

The contents of the Flash Drive will be confirmed by the IW before placing each of them inside the original and the duplicate audit bundles.

### **5. Configuration review of the Physical Access Control System and Intrusion Detection System (by SA)**

SA's attestation and hard copies of the screen shots and configuration audit log from the review process. See Appendix D on page 52.

### **6. Configuration review of the Firewall System (by SA)**

SA's attestation and hard copies of the firewall configuration from the review process. See Appendix E on page 53. Ensure the scrambled passwords are eliminated from the configuration before publishing it.

### **7. Other items**

If applicable.

## Appendix C: Key Ceremony Script (by IW)

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

IW: **Andy Newton**

Signature:

\_\_\_\_\_

Date: 2023 Nov \_\_

## Appendix D: Access Control System Configuration Review (by SA)

In my review of the KMF's Access Control System, I attest that the following are true and correct to the best of my knowledge:

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

Below are the reports that were generated from the access control system:

- 1. List of Personnel with assigned Access Group.
- 2. Configuration of Areas and Access Groups.
- 3. Logs for Access Event activities and Configuration activities.

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

SA:

\_\_\_\_\_

Signature:

\_\_\_\_\_

Date: 2023 Nov \_\_

## Appendix E: Firewall Configuration Review (by SA)

I have reviewed and confirmed that the firewall configuration satisfies the requirements of the DNSSEC Practice Statement with version 6th Edition (2020-11-04). No part of the signer system making use of the Hardware Security Module (HSM) is connected to any communication network.

SA:

\_\_\_\_\_

Signature:

\_\_\_\_\_

Date: 2023 Nov \_\_