

Root DNSSEC KSK Ceremony 42

Thursday 11 February 2021

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

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

Abbreviations

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

Participants

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

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

Title / Roles	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		2021 Feb —	
IW	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Hilary Jin / ICANN			
SA	Patrick Tudor / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			

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

Instructions for a Root DNSSEC KSK Ceremony

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

Ceremony Guidelines:

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

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony and Retrieve Materials

The CA initiates the ceremony by performing the steps below:

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

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

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

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms with SA that all audit cameras are recording and online video streaming is enabled.		
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.		
4	CA confirms that additional required personnel including COs, RZM, and Auditors are connected to the remote call. Scheduled remote participants are: CO4: Carlos Martinez (Key scripted for use) CO5: Olafur Gudmundsson (Key scripted for use) CO6: Nicolas Antoniello (Key scripted for use) CO3: Joao Damas (Key designated as backup) RZM: Duane Wessels / Verisign RZM: Trevor Davis / Verisign AUD: Elvin Paik / RSM		

Emergency Evacuation Procedures and Electronics Policy

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

Verify the Time and Date

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

Crypto Officer Key Verification

Step	Activity	Initials	Time
9	<p>The CA performs the following steps to verify the listed CO keys:</p> <ul style="list-style-type: none"> a) Remove the TEB from the shipping envelope and discard the shipping envelope. b) Inspect the TEB for tamper evidence. c) Read aloud the TEB number and place the TEB on the ceremony table visible to the audit camera. d) Open the TEB and place its contents on the ceremony table. e) Give the CO key declaration to IW to verify the CO key TEB number then insert the declaration into the audit bundle. f) Discard the TEB. g) Remove the CO tenant key from the padded envelope, and set the envelope aside for return shipping post-ceremony. h) Give the CO tenant key to the IW. <p>CO4: Carlos Martinez Key TEB # BB91951329 (See Appendix F on page 35)</p> <p>CO5: Olafur Gudmundsson Key TEB # BB91951327 (See Appendix G on page 36)</p> <p>CO6: Nicolas Antonello Key TEB # BB91951323 (See Appendix H on page 37)</p> <p>Note 1: The CO3 Joao Damas Safe Deposit Box Key TEB # BB91951330 has been designated as a backup. See Appendix I on page 38.</p> <p>Note 2: The COs' tenant keys were individually transmitted to separate trusted ICANN/PTI staff in advance due to invocation of disaster recovery procedures.</p>		

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
10	CA and IW transport a flashlight, and escort SSC2 into Tier 5 (Safe Room.)		
11	<p>SSC2 opens Safe #2 while shielding the combination from the camera.</p> <p>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.</p>		
12	<p>Perform the following steps to complete the safe log:</p> <ul style="list-style-type: none"> a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it. 		

Extract CO Credentials from Safe Deposit Boxes (Tier 7)

Step	Activity	Initials	Time
13	<p>IW performs the following steps sequentially to retrieve the required TEBs:</p> <ul style="list-style-type: none"> a) IW announces the name of the CO whose credentials will be extracted and requests their authorization to open their assigned safe deposit box. b) After the CO provides authorization, the CA operates the guard key in the bottom lock, then the IW uses the CO's tenant key to operate the top lock and opens their assigned safe deposit box. c) IW reads aloud the safe deposit box number, verifies its integrity, then removes the OP TEB and SO TEB. d) IW reads aloud the TEB numbers, then verifies integrity of TEBs while showing them to the audit camera above. e) IW retains the TEB(s) specified below, returns any TEBs not required, then closes and locks the safe deposit box with assistance from the CA. f) IW writes the date and time, then signs the safe log where "Remove" is indicated. g) CA verifies the completed safe log entries, then initials it. <p>CO4: Carlos Martinez Box # 1068 OP TEB # BB91951363 (Retain) SO TEB # BB46584665 (Check and Return)</p> <p>CO5: Olafur Gudmundsson Box # 1789 OP TEB # BB91951362 (Retain) SO TEB # BB46584381 (Check and Return)</p> <p>CO6: Nicolas Antonello Box # 1073 OP TEB # BB91951361 (Retain) SO TEB # BB46584383 (Check and Return)</p>		

Close Safe #2 (Tier 6, Credentials Safe)

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

Open Safe #1 (Tier 6, Equipment Safe)

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

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

Step	Activity	Initials	Time
21	<p>CA performs the following steps to extract each piece of equipment from the safe:</p> <ul style="list-style-type: none"> a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified in the list below. d) Write the date, time, and signature on the safe log where "Remove" is indicated. e) IW verifies the safe log entry, then initials it. <p>HSM3: TEB # BB51184234 (Check and Return) <i>Last Verified: KSK Ceremony 40-AC 2020-02-16</i></p> <p>HSM4: TEB # BB51184238 (Place on Cart) <i>Last Verified: KSK Ceremony 40 2020-02-16</i></p> <p>HSM5W: TEB # BB51184239 (Check and Return) <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>Laptop3: TEB # BB81420121 (Check and Return) <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>Laptop4: TEB # BB81420119 (Place on Cart) <i>Last Verified: KSK Ceremony 40 2020-02-16</i></p> <p>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384 (Place on Cart) <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p>KSK-2017: TEB # BB46584387 (Check and Return) <i>Last Verified: KSK Ceremony 38 2019-08-14</i></p> <p><i>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.</i></p>		

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

Step	Activity	Initials	Time
22	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the safe log entry then initials it.		
23	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.		
24	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 DVD (the laptop has no permanent storage device)
- Set up the printer
- Synchronize the laptop date and time
- Connect the HSMFD
- Start the log sessions
- Power ON the HSM (Tier 7)

Laptop Setup

Step	Activity	Initials	Time
1	<p>CA performs the following steps to prepare the listed equipment:</p> <ol style="list-style-type: none"> a) Remove all equipment TEBs from the cart and place them on the ceremony table. b) Inspect each equipment TEB for tamper evidence. c) Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB, then place the equipment on its designated area of the ceremony table. <p>HSM4: TEB # BB51184238 / Serial # H1411006 <i>Last Verified: KSK Ceremony 40 2020-02-16</i> Laptop4: TEB # BB81420119 / Service Tag # F8SVSG2 <i>Last Verified: KSK Ceremony 40 2020-02-16</i> OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951384 <i>Last Verified: KSK Ceremony 41 2020-04-23</i></p> <p><i>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.</i></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"> a) Open the latch on the right side of the laptop to confirm that the hard drive slot is empty. b) Open the latch on the left side of the laptop to confirm that the battery slot is empty. 		
3	<p>CA performs the following steps to boot the laptop:</p> <ol style="list-style-type: none"> a) Connect the USB printer cable into the rear USB port of the laptop. b) Connect the null modem cable into the serial port of the laptop. c) Connect the external HDMI display cable. d) Connect the power supply. e) Immediately insert the OS DVD release coen-0.4.0 after the laptop power is switched ON. 		
4	<p>CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the View menu and select Zoom In or Zoom Out To change the resolution of each screen: Go to Applications > Settings > Display</p>		

OS DVD Checksum Verification

Step	Activity	Initials	Time
5	<p>CA uses the terminal window to executes the following steps:</p> <ul style="list-style-type: none"> a) Calculate the SHA-256 hash by executing: <code>sha2wordlist < /dev/sr0</code> b) IW and participants confirm that the result matches the PGP Wordlist of the SHA-256 hash. <p>Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.</p> <p>SHA-256 hash: 8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f</p> <p>PGP Words: minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document</p> <p>Note: The SHA-256 hash of the OS DVD release coen-0.4.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/42</p>		

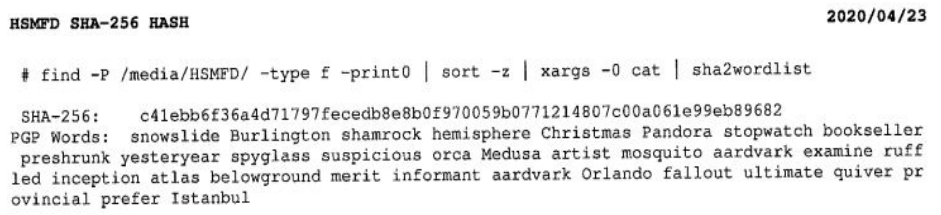
Printer Setup

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

Date Setup

Step	Activity	Initials	Time
7	<p>CA executes <code>date</code> using the terminal window to verify if the date/time reasonably matches the ceremony clock.</p> <p>If the date/time do not match, perform the following steps:</p> <ul style="list-style-type: none"> a) Execute <code>date -s "20210211 HH:MM:00"</code> to set the time. where HH is two-digit hour, MM is two-digit minutes and 00 is zero seconds. b) Execute <code>date</code> to confirm the date/time matches the clock. 		

Connect the HSMFD

Step	Activity	Initials	Time
8	CA plugs the Ceremony 41 HSMFD into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Display the HSMFD contents to all participants. c) Close the file system window.		
9	CA executes the command below using the terminal window to calculate the SHA-256 hash of the HSMFD: hsmfd-hash -c CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash with the following image from the previous ceremony script.  <p>The screenshot shows the following terminal output:</p> <pre>HSMFD SHA-256 HASH 2020/04/23 # find -P /media/HSMFD/ -type f -print0 sort -z xargs -0 cat sha2wordlist SHA-256: c41ebb6f36a4d71797fecedb8e8b0f970059b0771214807c00a061e99eb89682 PGP Words: snowslide Burlington shamrock hemisphere Christmas Pandora stopwatch bookseller preshrunk yesteryear spyglass suspicious orca Medusa artist mosquito aardvark examine ruff led inception atlas belowground merit informant aardvark Orlando fallout ultimate quiver pr ovincial prefer Istanbul</pre> IW confirms that the result matches the SHA-256 hash of the HSMFD from the Ceremony 41 annotated script.		

Distribute Previous HSMFD

Step	Activity	Initials	Time
10	CA gives the unused HSMFD 41 and the sheet of paper with the printed HSMFD hash to RKOS.		

Start the Terminal Session Logging

Step	Activity	Initials	Time
11	CA executes the command below using the terminal window to change the working directory to HSMFD: cd /media/HSMFD		
12	CA executes the command below to log activities of the Commands terminal window: script script-20210211.log		

Start the HSM Activity Logging

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

Power ON the HSM (Tier 7)

Step	Activity	Initials	Time
14	<p>CA performs the following steps to prepare the HSM:</p> <ul style="list-style-type: none"> a) Verify the label on the HSM reads HSM4 b) Ensure an RJ45 blockout is present in the "MGMT" port of the HSM. Install one if not present. c) Plug the null modem cable into the serial port of the HSM. d) Connect the power to the HSM, then switch it ON. <p>Note: Status information should appear on the HSM activity logging screen.</p> <ul style="list-style-type: none"> e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads H1411006, then scroll back to the bottom. <p>HSM4: Serial # H1411006</p> <p>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</p>		

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

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

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

Crypto Officer Credentials Verification

Step	Activity	Initials	Time
1	<p>CA performs the following steps to verify the COs' credentials:</p> <ul style="list-style-type: none"> a) Read aloud the TEB number, then inspect it for tamper evidence. b) Open the TEB, then remove the plastic case containing the card(s). c) Open the plastic case, then place the enclosed card(s) on the designated card holder at the front of the ceremony table. CA retains the plastic case on the ceremony table. <p>CO4: Carlos Martinez OP TEB # BB91951363</p> <p>CO5: Olafur Gudmundsson OP TEB # BB91951362</p> <p>CO6: Nicolas Antonello OP TEB # BB91951361</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"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "1.Set Online", press ENT to confirm. c) When "Set Online?" is displayed, press ENT to confirm. d) When "Insert Card OP #X?" is displayed, insert the OP card. e) When "PIN?" is displayed, enter "11223344", then press ENT. f) When "Remove Card?" is displayed, remove the OP card. g) Repeat steps d) to f) for the 2nd and 3rd OP cards. <p>Confirm the "READY" LED on the HSM is ON. IW records which cards were used below. Each card is returned to its designated card holder after use.</p> <p>1st OP card ____ of 7 2nd OP card ____ of 7 3rd OP card ____ of 7</p> <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</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	CA performs the following steps to test the network connectivity between laptop and HSM: a) Use the Commands terminal window b) Test connectivity by executing: ping hsm c) Wait for responses, then exit by pressing: Ctrl + C		

Insert the KSRFD

Step	Activity	Initials	Time
5	CA plugs the FD labeled " KSR " into an available USB port, then waits for it to be recognized by the OS. CA points out any KSR file that will be signed, then closes the file system window. Note: The KSRFD was transferred to the facility by the RKOS. It contains 3 KSRs. The first for the next calendar quarter and the remainder for subsequent quarter(s).		

Execute the KSR Signer for KSR 2021 Q2

Step	Activity	Initials	Time
6	CA executes the command below in the terminal window to sign the KSR file: <code>ksrsigner /media/KSR/KSK42-2021-Q2/ksr-root-2021-q2-0.xml</code>		
7	When the KSR signer displays the prompt: Activate HSM prior to accepting in the affirmative!! (y/N) : CA confirms that the HSM is online, then enters " y " to proceed.		

Verify the KSR Hash for KSR 2021 Q2

Step	Activity	Initials	Time
8	<p>When the hash of the KSR is displayed in the terminal window, perform the following:</p> <p>a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves. The IW verifies their employment documents and identification off camera for the purpose of authentication while maintaining privacy.</p> <p>Note: If the RZM representative is not physically present in the room, write the representative's name and "Remote Participant" next to the name on the signature line.</p> <p>b) IW retains the hash and PGP word list for the KSR(s), and employment verification letter provided by the RZM representative and writes their name on the following line:</p> <p>Note: If the RZM representative is not physically present in the room, the documents will be provided to RKOS in advance to be included in the final annotated script and audit bundle.</p> <p>_____</p> <p>c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.</p>		
9	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks "are there any objections?"		
10	CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSR/KSK42-2021-Q2/skr-root-2021-q2-0.xml</code>		

Execute the KSR Signer for KSR 2021 Q3

Step	Activity	Initials	Time
11	CA executes the command below in the terminal window to copy the previous quarter's generated SKR to construct a chain of trust to the subsequent KSR: <code>cp /media/KSR/KSK42-2021-Q2/skr-root-2021-q2-0.xml /media/KSR/KSK42-2021-Q3/skr.xml</code>		
12	CA executes the command below in the terminal window to sign the KSR file: <code>ksrsigner /media/KSR/KSK42-2021-Q3/ksr-root-2021-q3-0.xml</code>		
	Note: It is anticipated that the KSR Signer Software will issue a warning if one or more of the request's signatures will exceed the limit of 180 days of expiration in the future. All SKRs will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set will not expire more than 180 days in the future.		
13	When the KSR signer displays the prompt: Activate HSM prior to accepting in the affirmative!! (y/N) : CA confirms that the HSM is online, then enters "y" to proceed.		

Verify the KSR Hash for KSR 2021 Q3

Step	Activity	Initials	Time
14	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.		
15	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks " are there any objections? "		
16	CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSR/KSK42-2021-Q3/skr-root-2021-q3-0.xml</code>		

Execute the KSR Signer for KSR 2021 Q4

Step	Activity	Initials	Time
17	CA executes the command below in the terminal window to copy the previous quarter's generated SKR to construct a chain of trust to the subsequent KSR: <code>cp /media/KSR/KSK42-2021-Q3/skr-root-2021-q3-0.xml /media/KSR/KSK42-2021-Q4/skr.xml</code>		
18	CA executes the command below in the terminal window to sign the KSR file: <code>ksrsigner /media/KSR/KSK42-2021-Q4/ksr-root-2021-q4-0.xml</code> Note: It is anticipated that the KSR Signer Software will issue a warning if one or more of the request's signatures will exceed the limit of 180 days of expiration in the future. All SKRs will remain in the possession of the RZ KSK Operator until the time in which all RRSIG records in the set will not expire more than 180 days in the future.		
19	When the KSR signer displays the prompt: Activate HSM prior to accepting in the affirmative!! (y/N) : CA confirms that the HSM is online, then enters "y" to proceed.		

Verify the KSR Hash for KSR 2021 Q4

Step	Activity	Initials	Time
20	When the application requests verification of the KSR hash, the CA asks the RZM representative to read aloud the PGP word list SHA-256 hash of the KSR file sent to the Root Zone KSK Operator.		
21	Participants confirm that the hash displayed on the terminal window matches with the RZM representative's discourse, then CA asks " are there any objections? "		
22	CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSR/KSK42-2021-Q4/skr-root-2021-q4-0.xml</code>		

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
23	CA executes the commands below using the terminal window to print the KSR Signer log: a) <code>lpadmin -p HP -o copies-default=X</code> Note: Replace "X" with the amount of copies needed for the participants. b) <code>for i in \$(ls -l ksrsigner-202102*.log); do printlog \$i; done</code>		
24	IW attaches a copy of the required ksrsigner log to their script.		

Back up the Newly Created SKR

Step	Activity	Initials	Time
25	<p>CA executes the following commands using the terminal window:</p> <p>a) List the contents of the KSRFD by executing: <code>ls -ltrR /media/KSR</code></p> <p>b) Copy the contents of the KSRFD to the HSMFD by executing: <code>cp -pR /media/KSR/* .</code></p> <p>Note: Confirm overwrite by entering "y" if prompted.</p> <p>c) List the contents of the HSMFD to verify it has been copied successfully by executing: <code>ls -ltrR</code></p> <p>d) Unmount the KSRFD by executing: <code>umount /media/KSR</code></p>		
26	CA removes the KSRFD containing the SKR files, then gives it to RKOS.		

Disable/Deactivate the HSM (Tier 7)

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

Place the HSM (Tier 7) into a TEB

Step	Activity	Initials	Time
28	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.		
29	CA places the HSM into a prepared TEB, then seals it.		
30	CA performs the following steps: <ul style="list-style-type: none"> a) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and HSM serial number match below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM TEB on the cart. HSM4: TEB # BB51184285 / Serial # H1411006		

Act 4: Secure Hardware

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

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

Stop logging the Serial Output and the Terminal Session

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

Prepare blank FDs and back up the HSMFD Contents

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

Print Logging Information

Step	Activity	Initials	Time
15	<p>CA executes the following commands using the terminal window to print a copy of the logging information:</p> <ul style="list-style-type: none"> a) <code>lpadmin -p HP -o copies-default=1 -o fit-to-page-default=true</code> b) <code>enscript -2Gr script-202102*.log</code> c) <code>enscript -Gr --font="Courier8" ttyaudit-tty*-202102*.log</code> <p>Attach the printed copies to IW script. Note: Ignore the error regarding non-printable characters if prompted.</p>		

Place HSMFDs and OS DVDs into a TEB

Step	Activity	Initials	Time
16	<p>CA executes the following commands using the terminal window to unmount the HSMFD:</p> <ul style="list-style-type: none"> a) <code>cd /tmp</code> b) <code>umount /media/HSMFD</code> <p>CA removes the HSMFD, then places it on the holder.</p>		
17	<p>CA performs the following steps to switch OFF the laptop and remove the OS DVD:</p> <ul style="list-style-type: none"> a) Remove the OS DVD from the laptop. b) Turn OFF the laptop by pressing the power button. c) Disconnect all connections from the laptop. 		
18	CA places 2 HSMFDs, 2 OS DVDs, and 1 sheet of paper with the printed HSMFD hash into a prepared TEB, then seals it.		
19	<p>CA performs the following steps to verify the TEB:</p> <ul style="list-style-type: none"> a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the OS DVD TEB on the cart. <p>OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951322</p>		
20	<p>CA distributes the remaining HSMFDs:</p> <ul style="list-style-type: none"> 2 for IW (for audit bundles). 2 for RKOS (for SKR exchange with RZM and process review). 		

Place the Laptop into a TEB

Step	Activity	Initials	Time
21	CA places the laptop into a prepared TEB, then seals it.		
22	<p>CA performs the following steps:</p> <ul style="list-style-type: none"> a) Read aloud the TEB number and laptop serial number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number and laptop serial number matches with the information below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Place the laptop TEB on the cart. <p>Laptop4: TEB # BB81420089 / Service Tag # F8SVSG2</p>		

Place Crypto Officers' Credentials into TEBs

Step	Activity	Initials	Time
23	<p>CA perform the following steps sequentially for the COs listed below:</p> <ul style="list-style-type: none"> a) Gather the OP TEB and plastic case prepared for the CO. b) Take the CO's OP card from the card holder and place it inside of the plastic case. c) Place the plastic case into the prepared TEB, read aloud the TEB number and description, then seal it. d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory. e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. f) IW writes the date and time, then signs the table of IW's script, then CA initials the entry. g) IW places the TEBs on the ceremony table. h) Repeat steps for the remaining COs' credentials on the list. <p>CO4: Carlos Martinez OP TEB # BB91951297</p> <p>CO5: Olafur Gudmundsson OP TEB # BB91951296</p> <p>CO6: Nicolas Antoniello OP TEB # BB91951295</p>		

CO	Card Type	TEB #	Printed Name	Signature	Date	Time	CA Initials
CO4	OP 4 of 7	OP TEB # BB91951297	Yuko Green		2021 Feb __		
CO5	OP 5 of 7	OP TEB # BB91951296	Yuko Green		2021 Feb __		
CO6	OP 6 of 7	OP TEB # BB91951295	Yuko Green		2021 Feb __		

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

Step	Activity	Initials	Time
24	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
25	SSC1 opens Safe #1 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.		
26	SSC1 removes the safe log, then writes the date and time, then signs the safe log where " Open Safe " is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		
27	CA performs the following steps to return each piece of equipment to the safe: <ul style="list-style-type: none"> a) CAREFULLY remove the equipment TEB from the cart. b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1 c) Write the date, time, and signature on the safe log where "Return" is indicated. d) IW verifies the safe log entry, then initials it. <p>HSM4: TEB # BB51184285 Laptop4: TEB # BB81420089 OS DVD (release coen-0.4.0) + HSMFD: TEB # BB91951322</p>		

Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
28	SSC1 writes the date and time, then signs the safe log where " Close Safe " is indicated. IW verifies the entry, then initials it.		
29	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the " WAIT " light indicator is off.		
30	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
31	CA and IW transport a flashlight, and escort SSC2 into Tier 5 (Safe Room.)		
32	SSC2 opens Safe #2 while shielding the combination from the camera. Note: SSC begins by rapidly spinning the dial counter-clockwise 15-20 revolutions in order to charge it before stopping at the first number in the combination.		
33	SSC2 removes the safe log, then writes the date and time, then signs the safe log where " Open Safe " is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		

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

Step	Activity	Initials	Time
34	<p>IW performs the following steps sequentially to return the required TEBs:</p> <ul style="list-style-type: none"> a) IW reads aloud the TEB number, then verifies the integrity of the TEB while showing it to the audit camera above b) After the CA operates the guard key in the bottom lock, IW uses the CO's tenant key to operate the top lock and opens the CO's safe deposit box. c) IW reads aloud the safe deposit box number, places the TEB inside, then closes and locks the safe deposit box with assistance from the CA. d) IW writes the date and time, then signs the safe log where "Return" is indicated. e) CA verifies the completed safe log entry, then initials it. <p>CO4: Carlos Martinez Box # 1068 OP TEB # BB91951297</p> <p>CO5: Olafur Gudmundsson Box # 1789 OP TEB # BB91951296</p> <p>CO6: Nicolas Antoniello Box # 1073 OP TEB # BB91951295</p>		

Close Safe #2 (Tier 6, Credentials Safe)

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

Place Crypto Officer Keys into TEBs

Step	Activity	Initials	Time
38	<p>CA performs the following steps sequentially for the COs key listed below:</p> <ul style="list-style-type: none"> a) Gather the CO key TEB and envelope prepared for the CO. b) IW gives the CO key to CA who then places it inside of the envelope. c) Place the envelope into the prepared TEB, read aloud the TEB number and description, then seal it. d) Initial the TEB with a ballpoint pen, and give IW the sealing strips for post-ceremony inventory. e) IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen. f) Repeat steps for remaining COs' keys on the list. <p>CO4: Carlos Martinez Key TEB # BB91951299</p> <p>CO5: Olafur Gudmundsson Key TEB # BB91951298</p> <p>CO6: Nicolas Antoniello Key TEB # BB91951293</p> <p>Note: The COs' keys will be promptly returned to the COs who will sign a second key declaration form confirming receipt. The completed declaration forms will be available on the IANA web page along with the standard post-ceremony materials.</p>		

Act 5: 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 asks any COs who are participating remotely if they have any concerns pertaining to the ceremony or exceptions which may have occurred.		
3	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. All signatories declare that this script is a true and accurate record of the ceremony.		
4	CA reviews IW's script, then signs the participants list.		
5	IW signs the list and records the completion time.		

Stop Online Streaming and Post Ceremony Information

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

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

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

Bundle Audit Materials

Step	Activity	Initials	Time
12	<p>IW makes a copy of their script for off-site audit bundle containing:</p> <ul style="list-style-type: none"> a) Output of signer system – HSMFD. b) Copy of IW's key ceremony script. c) Audio-visual recording from the audit cameras. d) Logs from the Physical Access Control System and Intrusion Detection System: Range: 20200423 00:00:00 to 20210212 00:00:00 UTC e) IW's attestation (See Appendix C on page 32). f) SA's attestation (See Appendix D on page 33 and Appendix E on page 34). <p>All TEBs are labeled Root DNSSEC KSK Ceremony 42, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>		

Appendix A: References

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

- [1] **coen**: The Ceremony Operating ENvironment (COEN) is a *Reproducible* ISO image consisting of a live operating system.
More information and the OS image source code can be found at <https://github.com/iana-org/coen>
- [2] **sha2wordlist**: Is an application written in C by Kirei AB, which digests STDIN and output a SHA-256 checksum displayed as PGP words.
The source code is available at <https://github.com/kirei/sha2wordlist>
- [3] **configure-printer**: Is a bash script used to install the HP LaserJet printer from the command line instead using system-config-printer.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*
- [4] **hsmfd-hash**: Is a bash script used to calculate, print and compare SHA-256 checksums for the HSMFD flash drives. It has the following options:
 - a) **-c** Calculate the HSMFD SHA-256 hash and PGP Word List
 - b) **-p** Print the calculated HSMFD SHA-256 hash and PGP Word List using the default printer
 - c) **-m** Compare the calculated SHA-256 hashes between HSMFDs

The following is the main command invoked by this script:

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

Note: The sort command has a different behavior depending on the locale settings specified in environment variables. Current OS locale setting is `LC_COLLATE="POSIX"`

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

- [5] **ttyaudit**: Is a perl script use to capture and logging the *HSM* output.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*
- [6] **ping hsm**: The HSM static IP address `192.168.0.2` has been included in the `/etc/hosts` file.
- [7] **ksrsigner**: Is an application written in C by Dr. Richard Lamb, which uses the KSK private key stored in the HSM to generate digital signatures for the ZSK.
The source code is available at <https://github.com/iana-org/dnssec-keytools>
- [8] **printlog**: Is a bash script use to print the *Key Signing Log* output from **ksrsigner** application.
The source code is available at https://github.com/iana-org/coen/blob/master/tools/packages/ksk-tools-0.1.0coen_amd64.deb*

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

Appendix B: Audit Bundle Checklist

1. Output of Signer System (by CA)

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

2. Key Ceremony Script (by IW)

Hard copies of the IW's key ceremony script, notes during the ceremony and attestation. See Appendix C on page 32.

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 33.

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 34. 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: **Yuko Green**

Signature:

Date: 2021 Feb __

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: **20200423 00:00:00 to 20210212 00:00:00 UTC.**

SA:

Signature:

Date: 2021 Feb __

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.

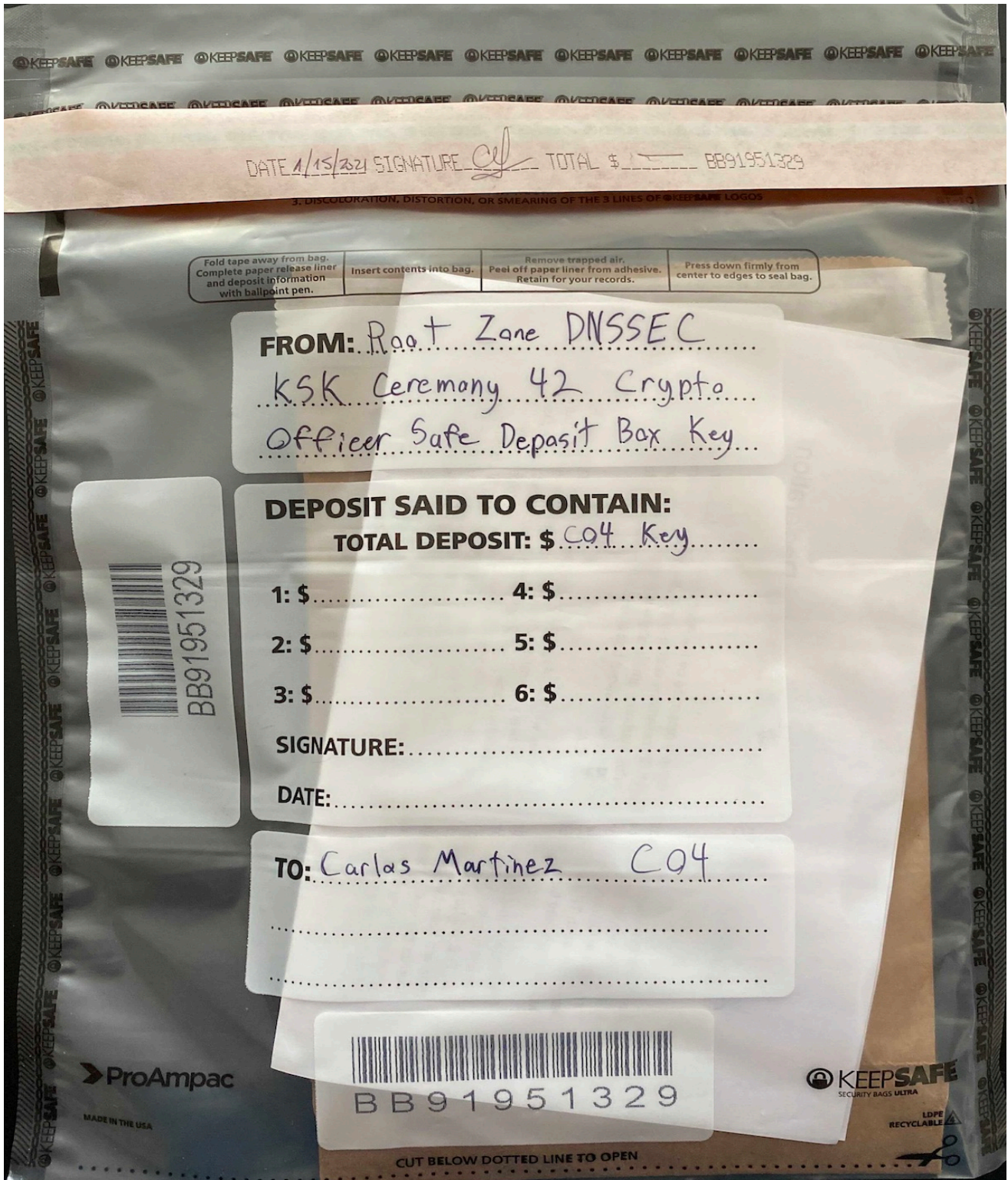
SA:

Signature:

Date: 2021 Feb __

Appendix F: CO4 Safe Deposit Box Key Chain of Custody

The following photo contains the CO4 Carlos Martinez Safe Deposit Box Key TEB # BB91951329 dispatched from the CO.



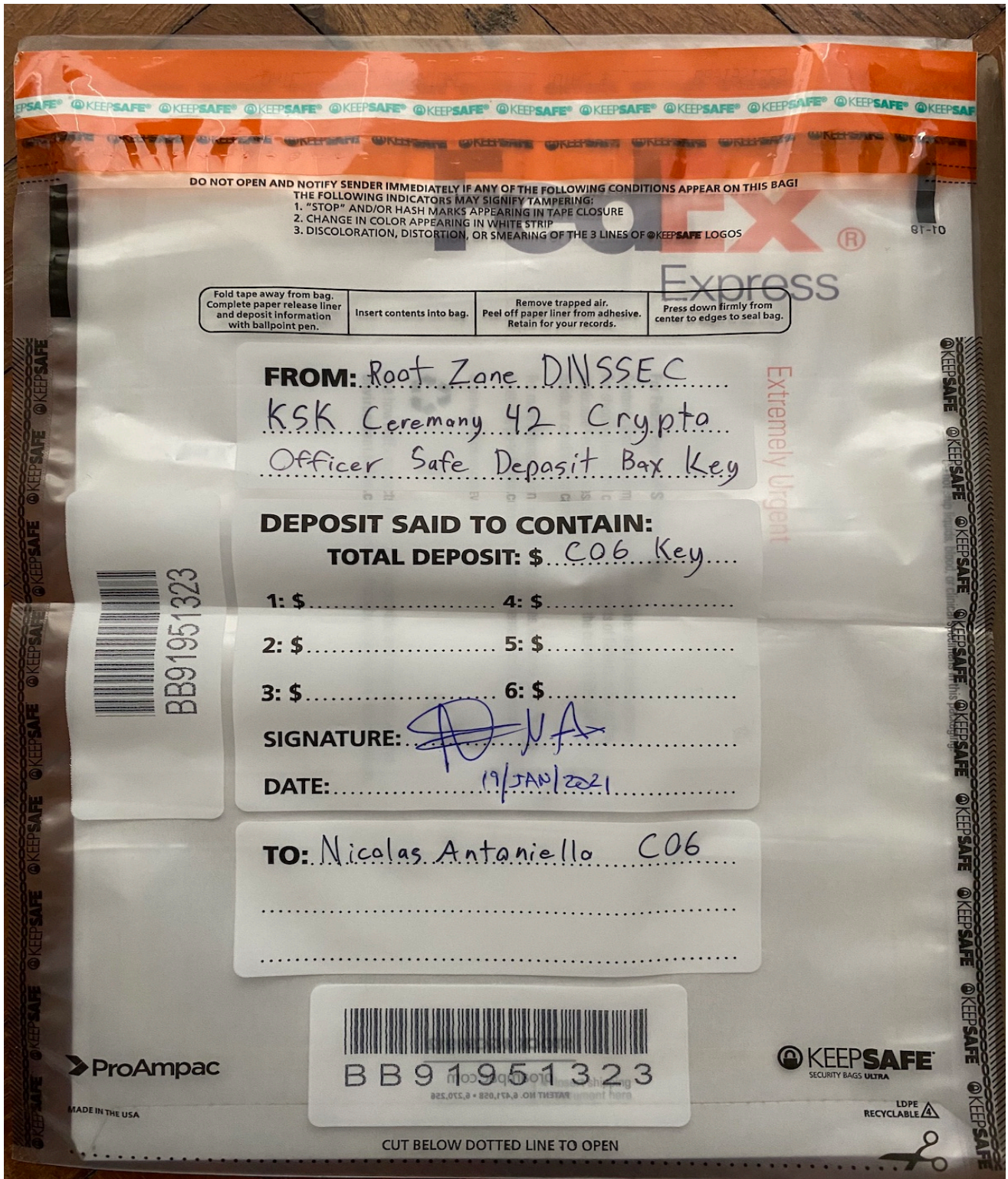
Appendix G: CO5 Safe Deposit Box Key Chain of Custody

The following photo contains the **CO5 Olafur Gudmundsson Safe Deposit Box Key TEB # BB91951327** dispatched from the CO.



Appendix H: CO6 Safe Deposit Box Key Chain of Custody

The following photo contains the CO6 Nicolas Antoniello Safe Deposit Box Key TEB # BB91951323 dispatched from the CO.



Appendix I: CO3 Safe Deposit Box Key Chain of Custody

The following photo contains the CO3 Joao Damas Safe Deposit Box Key TEB # BB91951330 dispatched from the CO.

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

