

Root DNSSEC KSK

Administrative Ceremony
HSM Acceptance Testing

Wednesday 13 October 2021

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

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


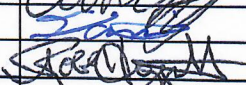
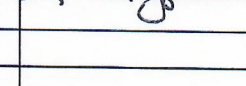

Abbreviations

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 the time of completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Matthew Larson / ICANN		2021 Oct 13	15:12
IW	Aaron Foley / PTI			
SSC1	Fernanda Iunes / ICANN			
SW	Robert Hoggarth / ICANN			

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 Administrative Ceremony

The Root DNSSEC Key Signing Key (KSK) Administrative Ceremony is a scripted meeting where individuals with specific roles perform tasks related to support the operation of the Root Zone KSK. Administrative Ceremonies include all ceremonies that do not require use of the private key component of the root zone DNSSEC KSK, such as enrollment or replacement of a trusted role, media deposit or extraction, equipment acceptance testing or maintenance, etc. 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

The CA initiates the ceremony by performing the steps below:

- Verify that the audit cameras are recording
- 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

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms that required audit cameras are recording.	<i>[Signature]</i>	14:00
2	CA confirms that all participants are signed into Tier 4 (Key Ceremony Room) log, then performs a roll call using the participants list on page 2.	<i>[Signature]</i>	14:00
3	CA asks that any first time ceremony participants in the room introduce themselves.	<i>[Signature]</i>	14:01

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.	<i>[Signature]</i>	14:01
5	CA explains the use of personal electronic devices during the ceremony.	<i>[Signature]</i>	14:01
6	CA summarizes the purpose of the ceremony.	<i>[Signature]</i>	14:02

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: <u>2021-10-13 14:02</u>	<i>[Signature]</i>	14:02
Note: All entries into this script or any logs should follow this common source of time.			

Act 2: HSM Acceptance Testing




The CA performs the HSM Acceptance Testing by executing the following steps:

- Inspect the HSM's Tamper Evident Bag for tamper evidence
- Set up and configure the testing laptop, peripherals, and connections
- Power on HSM
- Issue Security Officer (SO) cards and set HSM to secure state
- Issue Crypto Officer (CO) Operator (OP), and Adapter Authorization Key (AAK) cards
- Change and verify API settings
- Verify connectivity, activate, and initialize HSM
- Generate and verify a test key
- Erase / zeroize / unsecure HSM and power off
- Store the HSM inside of a Tamper Evident Bag
- Power off and disconnect remaining equipment
- Place HSM in Tier 6 (Equipment Safe #1)


Verify Chain of Custody

Step	Activity	Initials	Time
1	<p>CA performs the following steps to unbox the new HSM.</p> <p>a) Unpack the HSM box while leaving HSM enclosed in the vendor supplied TEB.</p> <p>b) Inspect the HSM vendor supplied TEB for tamper evidence.</p> <p>c) Match HSM serial number and vendor TEB to digitally signed email from the vendor (See Appendix A on page 19). If these do not match, re-package HSMs, terminate the ceremony, and return HSMs.</p> <p>d) Remove and discard the TEB, then place the HSM on its designated area of the ceremony table.</p> <p>e) Affix a label on the HSM.</p> <p>HSM6E: TEB # PS073428 / Serial # H2001001</p>		14:06
2	<p>CA removes the small packet on top of the HSM containing the HSM physical key and performs the following steps:</p> <p>a) Verify the serial number on the packet matches with the HSM serial number.</p> <p>b) Verify the number in the key matches with the number in the packet.</p> <p>c) Return the physical key to the small packet and set it aside for RKOS to store.</p> <p>Note: The HSM physical key is used to enable/disable the LCD display and the keypad.</p>		14:07


Laptop Setup

Step	Activity	Initials	Time
3	CA performs the following steps to confirm that no hard drive and battery are in the testing laptop: a) Confirm that the hard drive slot is empty. b) Confirm that the battery slot is empty.		14:07
4	CA performs the following steps to boot the testing laptop: a) Connect the null modem cable into the serial port of the laptop. b) Connect the external HDMI display cable. c) Connect the power supply. d) Immediately insert the copy of the OS DVD release coen-0.4.0 after the laptop power is switched ON.		14:10
5	CA verifies functionality of the external display and performs adjustments if necessary: To change the font size of the terminal: Click the View menu and select Zoom In or Zoom Out To change the resolution of each screen: Go to Applications > Settings > Display		14:12



OS DVD Checksum Verification

Step	Activity	Initials	Time
6	CA uses the terminal window to executes the following steps: 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. Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirms the hash from the ceremony script. SHA-256 hash: 8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f 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 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/43		14:14


Date Setup

Step	Activity	Initials	Time
7	CA executes <code>date</code> using the terminal window to verify if the date/time reasonably matches the ceremony clock. If the date/time do not match, perform the following steps: a) Execute <code>date -s "20211013 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.		14:15



Format and label the blank FD

Step	Activity	Initials	Time
8	CA performs the following steps to format a new FD: a) Plug a new FD into an available USB port in the laptop and wait for it to be recognized. b) Close the file system popup window. CA uses the terminal window to perform the following steps: c) Confirm the drive letter by executing: df d) Unmount the drive by executing: umount /dev/sdb1 e) Format and label the FD by executing: mkfs.vfat -n HSMFD -I /dev/sdb1 f) CA removes the FD, then places it on the holder.		14:17
9	CA repeats step 8 for the 2 nd blank FD.		14:17


Connect the HSMFD

Step	Activity	Initials	Time
10	CA plugs an empty HSMFD into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Close the file system window.		14:17

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		14:18
12	CA executes the command below to log activities of the Commands terminal window: script script-20211013.log		14:18

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.		14:19


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) Install an RJ45 blockout in the "MGMT" port of the HSM. b) Plug the null modem cable into the serial port of the HSM. c) Connect the power to the HSM, then switch it ON. <i>Note: Status information should appear on the HSM activity logging screen.</i> d) Scroll the logging screen up and locate the HSM serial number. e) Scroll up on the logging screen while IW verifies the displayed HSM serial number on the screen reads H2001001, then scroll back to the bottom. f) After the completion of the HSM self test the display should say "Important Read Manual" indicating the HSM is in the initialized state. <p>HSM6E: Serial # H2001001 <i>Note: The date and time on the HSM is not used as a reference for logging and timestamp.</i></p>	<i>CA</i>	14:22

Issue Security Officer (SO) Cards

Step	Activity	Initials	Time
15	<p>CA performs the following steps to issue Security Officer (SO) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "1.Issue SO Cards", press ENT to confirm. c) When "Issue SO Cards?" is displayed, press ENT to confirm. d) When "Num Cards?" is displayed, enter "2", then press ENT. e) When "Num Req Cards?" is displayed, enter "2", then press ENT. f) When "Insert Card #X?" is displayed, insert the required SO card. g) When "Remove Card?" is displayed, remove the SO card. h) Repeat steps f) to g) for the 2nd SO card. i) When "SO Cards Issued" is displayed, press ENT to confirm. <p><i>Note: If the card is unreadable, gently wipe its metal contacts and try again.</i></p>	<i>CA</i>	14:24

Configure the HSM to Secure State

Step	Activity	Initials	Time
16	<p>CA performs the following steps to configure the HSM to secure state using Security Officer (SO) cards:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "3.Secure", press ENT to confirm. c) When "Secure?" is displayed, press ENT to confirm. d) When "Insert Card SO #X?" is displayed, insert the SO card. e) When "PIN?" is displayed, enter "11223344", then press ENT. f) When "Remove Card?" is displayed, remove the SO card. g) Repeat steps d) to f) for the 2nd SO card. h) When "SMK AES Triple DES?" is displayed, press CLR to skip. i) When "SMK AES" is displayed, press ENT to confirm. j) When "LAN Port Number?" is displayed, press CLR to skip. k) When "Enable IPv4/IPv6?" is displayed, press CLR to skip. l) When "LAN IPv4 Address?" is displayed, press CLR to skip. m) When "LAN IPv4 Mask?" is displayed, press CLR to skip. n) When "Set IPv4 Gateway?" is displayed, press CLR to skip. o) When "LAN IPv6 Address?" is displayed, press CLR to skip. p) When "LAN IPv6 Mask?" is displayed, press CLR to skip. q) When "Set IPv6 Gateway?" is displayed, press CLR to skip. r) When "Remote Mgmt Off Enable?" is displayed, press CLR to skip. s) When "Remote Mgmt Off" is displayed, press ENT to confirm. t) When "Change Clock?" is displayed, press CLR to skip. u) When "Import Config?" is displayed, press CLR to skip. v) When "FIPS Mode On Disable?" is displayed, press CLR to skip. w) When "FIPS Mode On" is displayed, press ENT to confirm. x) When "Global Key Export Enabled" is displayed, press CLR to skip. <p>Done Rebooting Device will be displayed. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>		14:27



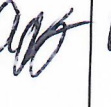
Root DNSSEC Script Exception

Exception Details


Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: <u>2</u> Step(s): <u>19</u> Page(s): <u>11</u> Date and Time: <u>2021 10 13</u>		
2.	IW describes the exception(s) and action(s) below.		

Step 19a assumes you are in the role management menu. The menu had to be selected and SO cards used to proceed to backup AAK

Issue Crypto Officer (CO), Operator (OP), and Adapter Authorization Key (AAK) Cards

Step	Activity	Initials	Time
17	<p>CA performs the following steps to issue Crypto Officer (CO) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "7.Role Mgmt", press ENT to confirm. When "Insert Card SO #X?" is displayed, insert the SO card. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the SO card. Repeat steps c) to e) for the 2nd SO card. Select "1.Issue Cards", press ENT to confirm. Select "1.Issue CO Cards", press ENT to confirm. When "Issue CO Cards?" is displayed, press ENT to confirm. When "Num Cards?" is displayed, enter "2", then press ENT. When "Num Req Cards?" is displayed, enter "2", then press ENT. When "Insert Card #X?" is displayed, insert the required CO card. When "Remove Card?" is displayed, remove the CO card. Repeat steps l) to m) for the 2nd CO card. When "CO Cards Issued" is displayed, press ENT to confirm. <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>		14:31
18	<p>CA performs the following steps to issue Operator (OP) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "2.Issue OP Cards", press ENT to confirm. When "Issue OP Cards?" is displayed, press ENT to confirm. When "Num Cards?" is displayed, enter "2", then press ENT. When "Num Req Cards?" is displayed, enter "2", then press ENT. When "Insert Card #X?" is displayed, insert the required OP card. When "Remove Card?" is displayed, remove the OP card. Repeat steps f) to g) for the 2nd OP card. When "OP Cards Issued" is displayed, press ENT to confirm. Press CLR twice to return to the main menu "Secured" <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>		14:33
19	<p>CA performs the following steps to issue Adapter Authorization Key (AAK) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "3.Backup AAK" from the same menu "Role Mgmt", press ENT to confirm. When "Backup AAK?" is displayed, press ENT to confirm. When "Num Cards?" is displayed, enter "2", then press ENT. When "Insert Card #X?" is displayed, insert the required AAK card. When "Remove Card?" is displayed, remove the AAK card. Repeat steps e) to f) for the 2nd AAK card. When "AAK Exported" is displayed, press ENT to confirm. Press CLR to return to the menu "Secured". <p>Each card is returned to its designated card holder after use. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>		14:40

Change the API Settings

Step	Activity	Initials	Time
20	<p>CA performs the following steps to change the API settings:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "5.Key Mgmt", press ENT to confirm. c) When "Insert CO Card #X?" is displayed, insert either CO card. d) When "PIN?" is displayed, enter "11223344", then press ENT. e) When "Remove Card?" is displayed, remove the CO card. f) Repeat steps c) to e) for the 2nd CO card. g) Select "5. API Settings", press ENT to confirm. h) Select "1.Key Import", press ENT to confirm. i) When "Key Import On Disable?" is displayed, press ENT to confirm. j) Select "2.Key Export", press ENT to confirm. k) When "Key Export On Disable?" is displayed, press ENT to confirm. l) Select "5.Sym Key Der", press ENT to confirm. m) When "Sym Key Der On Disable?" is displayed, press ENT to confirm. n) Press CLR to return to the menu "Key Mgmt" <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>		<p>14:42</p>



Verify the API Settings

Step	Activity	Initials	Time
21	<p>CA performs the following steps to dump the status of the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "8.HSM Info" from the same menu "Key Mgmt", press ENT to confirm. Select "8.Output Info", press ENT to confirm. When "Output Info?" is displayed, press ENT to confirm. Press CLR twice to return to the main menu "Secured" <p>CA selects the HSM Output terminal window and scrolls up to confirm with IW the output of the HSM configuration matches with the list below:</p> <pre> Modes: (1=Enabled 0=Disabled) Global Key Export 1 App Key Import 0 App Key Export 0 Asymmetric Key Gen 1 Symmetric Key Gen 1 Symmetric Key Derive 0 Signing 1 Signature Verify 1 MAC Generation 1 MAC Verification 1 Encrypt / Decrypt 1 Delete Asym Key 1 Delete Sym Key 1 Output Key Details 1 Output Key Summary 1 Suite B Algorithms 1 Non Suite B Algs 1 Auto Online 0 Remote Management 0 AES SMK Set Offline FIPS Mode </pre>	<i>CPG</i>	14:44


Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
22	<p>CA performs the following steps to activate the HSM:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "1.Set Online", press ENT to confirm. When "Set Online?" is displayed, press ENT to confirm. When "Insert Card OP #X?" is displayed, insert the OP card. When "PIN?" is displayed, enter "11223344", then press ENT. When "Remove Card?" is displayed, remove the OP card. Repeat steps d) to f) for the 2nd OP card. <p>Confirm the "READY" LED on the HSM is ON. Note: If the card is unreadable, gently wipe its metal contacts and try again.</p>	<i>CPG</i>	14:46


Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
23	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		14:46
24	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		14:47


Initialize HSM

Step	Activity	Initials	Time
25	CA performs the following steps to initialize the HSM: a) Set environment variables . /opt/dnssec/fixenv b) Execute: inittoken c) For the slot number enter: 0 d) For the PKCS11 Token name enter: ICANNTEST e) For the User PIN enter and re-enter: 123456 f) For Security Officer PIN enter and re-enter: 123456 g) This should return "Token initialised OK"		14:48

Generate New Test Key

Step	Activity	Initials	Time
26	CA executes the command below in the terminal window to generate new test key: kskgen When Activate HSM prior to accepting in the affirmative!! (y/N): CA confirms that the HSM is online, then enters "y" to proceed. If slot is asked type 0		14:49

Verify the Test KSK

Step	Activity	Initials	Time
27	CA checks the Test KSK by executing in to the terminal window: keybackup -l -P 123456 Verify the presence of the public and private keypair created previously by the kskgen command.		14:50

Erase / Zeroize / Unsecure HSM

Step	Activity	Initials	Time
28	CA selects the HSM Output terminal window. CA presses the RESTART button on the HSM to take OFFLINE and waits for SELF TEST to complete. Confirm the READY LED on the HSM is OFF .	<i>CPJ</i>	14:51
29	CA performs the following steps to return the HSM to Unsecure factory default state. This will erase all keys, settings, and configuration. <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "6.HSM Mgmt", press ENT to confirm. c) When "Insert Card SO #X?" is displayed, insert the SO card. d) When "PIN?" is displayed, enter "11223344", then press ENT. e) When "Remove Card?" is displayed, remove the SO card. f) Repeat steps c) to e) for the 2nd SO card. g) Select "5.Unsecure", press ENT to confirm. h) When "Unsecure?" is displayed, then press ENT. <p>Note: If the card is unreadable, gently wipe its metal contacts and try again.</p> <p>It may take a few minutes for the HSM to restart after the zeroization is complete.</p> <p>The HSM will reboot into the "Unsecured State" and after the completion of the HSM self test the display should say "Important Read Manual" indicating the HSM is in the initialized state.</p>	<i>CPJ</i>	14:53
30	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.	<i>CPJ</i>	14:53

Place HSM in the TEB

Step	Activity	Initials	Time
31	CA places the HSM into a prepared TEB, then seals it.	<i>CPJ</i>	14:54
32	CA performs the following steps to verify the TEB: <ul style="list-style-type: none"> a) Read aloud the TEB number and HSM serial number, then show the TEB to the audit camera above for participants to see. b) Confirm with IW that the TEB number and 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 HSM TEB on the cart. <p>HSM6E: TEB # BB51184245 / Serial # H2001001</p>	<i>CPJ</i>	14:55

Place SO, OP, CO, and AAK cards into a plastic case

Step	Activity	Initials	Time
33	CA places the SO, OP, CO, and AAK cards into a plastic case and sets it aside for use in future acceptance testing ceremonies.	<i>CPJ</i>	14:56

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
34	CA performs the following steps to stop logging: a) Perform the following steps using the HSM Output terminal window to stop logging the serial output (ttyaudit): i) Press Ctrl + C ii) Execute exit b) Execute the command below using the Commands terminal window to stop logging the terminal session: exit Note: The Commands terminal session window will remain open.	<i>CAJ</i>	14:57

Back up the HSMFD Contents

Step	Activity	Initials	Time
35	CA executes the command below using the terminal window to enable copying of all content from the HSMFD: shopt -s dotglob	<i>CAJ</i>	14:57
36	CA executes the command below using the terminal window to display the contents of the HSMFD: ls -ltrR	<i>CAJ</i>	14:58
37	CA plugs a blank FD labeled HSMFD into an available USB slot on the laptop, then waits for the OS to recognize it as HSMFD1	<i>CAJ</i>	14:58
38	CA closes the file system window, then executes the command below to back up the HSMFD: cp -pR * /media/HSMFD1	<i>CAJ</i>	14:59
39	CA executes the command below using the terminal window to compare the SHA-256 hash between the original HSMFD and the HSMFD copy: hsmfd-hash -m	<i>CAJ</i>	14:59
40	CA executes the command below using the terminal window to unmount the HSMFD copy: umount /media/HSMFD1	<i>CAJ</i>	14:59
41	CA removes the HSMFD1 , then places it on the holder.	<i>CAJ</i>	15:00

Power OFF the Laptop

Step	Activity	Initials	Time
42	CA performs the following steps: a) Executes the command below to unmount the HSMFD: i) cd /tmp ii) umount /media/HSMFD CA removes the HSMFD, then places it on the holder.	<i>CAJ</i>	15:00
43	CA performs the following steps to switch OFF the laptop and remove the OS DVD: 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.	<i>CAJ</i>	15:01

Open Equipment Safe #1

Step	Activity	Initials	Time
44	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		
45	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.	CAW	15:02
46	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. IW verifies this entry then initials it.	CAW	15:03
47	CA performs the following steps to place the HSM and HSM physical key into the Safe: a) CAREFULLY remove the equipment TEBs from the cart. b) Read aloud the TEB numbers while showing them to the audit camera above, then place them inside Safe #1 c) Write the date, time, and signature on the safe log where "Place" is indicated. d) IW verifies the safe log entry, then initials it. HSM6E: TEB # BB51184245 / Serial # H2001001	CAW	15:05
		CAW	15:07

Close Equipment Safe #1

Step	Activity	Initials	Time
48	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the entry, then initials it.	CAW	15:07
49	SSC1 returns the safe log back to Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	CAW	15:08
50	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	CAW	15:09

Act 3: Close the Administrative Ceremony

The CA will finish the ceremony by:

- Reading all exceptions that occurred during the ceremony
- Calling the ceremony participants to sign the IW's script
- Stopping the video recording
- Ensuring that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out
- Preparing the audit bundle materials

Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.	CA	15:09
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. All signatories declare that this script is a true and accurate record of the ceremony.	CA	15:11
3	CA reviews IW's script, then signs the participants list.	CA	15:12
4	IW signs the list and records the completion time.	IW	15:13

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

Step	Activity	Initials	Time
5	CA stops the audit camera video recording.	CA	15:13
6	CA and IW ensure that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room).	CA	15:15

Bundle Audit Materials

Step	Activity	Initials	Time
7	IW makes a copy of their script for off-site audit bundle containing: <ol style="list-style-type: none"> Copy of IW's administrative ceremony script. Audio-visual recording. IW's attestation (See Appendix D on page 22). <p>All TEBs are labeled Root DNSSEC Administrative Ceremony HSM Acceptance Testing, dated and signed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>	CA	17:23

Appendix A: HSM Chain of Custody

The following digitally signed email contains the HSM serial number and TEB number dispatched from the vendor.

Your order PO# 20JR71289 - Temporary Items

Message

Delete Reply Reply All Forward Attachment Meeting Move Junk Rules Read/Unread Categorize Follow Up

Your order PO# 20JR71289

PC Peter Clements <Peter.Clements@ultra-cis.com> Today at 08:27
 To: Andres Pavez; Cc: Gillian Marlor; Jasper Rose; Robin Allott; Adam Minter

This message was digitally signed by "Peter.Clements@ultra-cis.com".

Dear Andres,

Please find details of your order dispatched on 30/03/2020.

Recipient:

ICANN
 1920 East Maple Avenue
 El Segundo
 California
 CA 90245
 UNITED STATES

Your order has been dispatched please see details below:

Date	30/03/2020
Customer PO#	PO# 20JR71289
Ultra CIS Ref#	U1000645
Courier Used	Fed Ex
AWB/Tracking #	77012779270
Product Type	AEP-KEY-PLS

Serial Number	Tamper Bag Ref
H2001001	PS073428

Peter Clements
 Head of Compliance

View Certificate

USERTrust RSA Certification Authority
 Sectigo RSA Client Authentication and Secure Email CA
 peter.clements@ultra-cis.com

peter.clements@ultra-cis.com
 Issued by: Sectigo RSA Client Authentication and Secure Email CA
 Expires: Saturday, December 19, 2020 at 15:59:59 Pacific Standard Time
 This certificate is valid

Details

Subject Name
 Email Address peter.clements@ultra-cis.com

Issuer Name
 Country or Region GB
 State/Province Greater Manchester
 Locality Salford
 Organization Sectigo Limited
 Common Name Sectigo RSA Client Authentication and Secure Email CA

Serial Number 2B D7 E9 2D D1 29 B7 04 A1 02 E2 DB DF 93 AE 03
 Version 3
 Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
 Parameters None

OK

Appendix B: 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] **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*
- [4] **ping hsm**: The HSM static IP address `192.168.0.2` has been included in the `/etc/hosts` file.
- [5] **kskgen**: Is an application written in C by Dr. Richard Lamb, which create a KSK stored in the HSM.
The source code is available at <https://github.com/iana-org/dnssec-keytools>
- [6] **keybackup**: Is an application written in C by Dr. Richard Lamb, which list, delete, and backup keys.
The source code is available at <https://github.com/iana-org/dnssec-keytools>
- [7] **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) `-h` Show this *help* message
 - b) `-c` Calculate the HSMFD SHA-256 hash and PGP Word List
 - c) `-p` Print the calculated HSMFD SHA-256 hash and PGP Word List using the default printer
 - d) `-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*

* 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 C: Audit Bundle Checklist

1. Administrative Ceremony Script (by IW)

Hard copies of the IW's administrative ceremony script, including notes and attestation. See Appendix D on page 22.

2. Audio-Visual Recordings from the Administrative Ceremony (by CA)

One set of the audit camera footages.

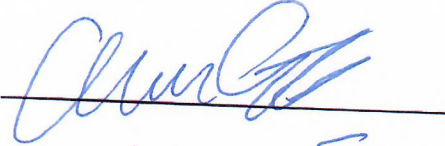
3. Other items

If applicable.

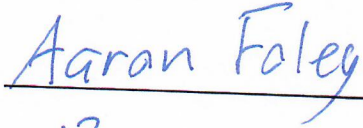
Appendix D: Administrative Ceremony Script (by IW)

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

IW:

A handwritten signature in blue ink, appearing to be 'Aaron Foley', written over a horizontal line.

Signature:

A handwritten signature in blue ink, clearly legible as 'Aaron Foley', written over a horizontal line.

Date: 2021 Oct 13