

Root DNSSEC KSK
Administrative Ceremony
HSM Acceptance Testing

Tuesday 13 February 2024

Root Zone KSK Operator Key Management Facility
1920 East Maple Avenue, El Segundo, CA 90245, 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
EW = External Witness
IW = Internal Witness
OP = Operator
RKOS = RZ KSK Operations Security
SKR = Signed Key Response
SSC = Safe Security Controller
TEB = Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20)



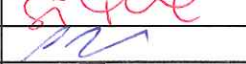



CA = Ceremony Administrator
FD = Flash Drive
KMF = Key Management Facility
PTI = Public Technical Identifiers
RZM = Root Zone Maintainer
SMK = Storage Master Key
SW = Staff Witness

CO = Crypto Officer
HSM = Hardware Security Module
KSR = Key Signing Request
RKSH = Recovery Key Share Holder
SA = System Administrator
SO = Security Officer
TCR = Trusted Community Representative

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	Andres Pavez / PTI		2024 Feb 13	19:05
IW	Aaron Foley / PTI			
SSC1	Sabrina Tanamal / PTI			
EW	Ralf Weber			
EW	Arbogast Fabian			
EW	Jorge Etges			

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 begins recording with the audit cameras shortly before the ceremony begins
- Ceremony participants follow the script step by step in order to attest to the ceremony's proper performance
- The CA reads each step aloud prior to its performance
- Upon the successful completion of a step, the IW will announce and record its time of completion, and initials that step in their script
- A ceremony participant who has cause for concern or detects an issue is encouraged to interrupt the ceremony for discussion. The issue is brought to resolution before the ceremony resumes
- Questions and suggestions for improvement are welcome and can be discussed at any time or after the ceremony during the ceremony debrief

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

Key Management Facility Tiers:

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

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

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

Act 1: Initiate Ceremony

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
- Explain the purpose of the ceremony along with a high-level list of tasks to be completed

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1.1	CA confirms that required audit cameras are recording.	<i>[Signature]</i>	17:51
1.2	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>	17:52
1.3	CA asks that any first-time ceremony participants in the room introduce themselves.	<i>[Signature]</i>	17:52

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
1.4	CA reviews emergency evacuation procedures with onsite participants.	<i>[Signature]</i>	17:53
1.5	CA explains the use of personal electronic devices during the ceremony.	<i>[Signature]</i>	17:53
1.6	CA summarizes the purpose of the ceremony.	<i>[Signature]</i>	17:53

Verify the Time and Date



Step	Activity	Initials	Time
1.7	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: <u>2024-02-13 17:55</u>	<i>[Signature]</i>	17:55
<p>Note: All entries into this script or any logs should follow this common source of time.</p>			

Act 2: HSM Acceptance Testing

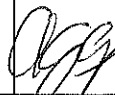

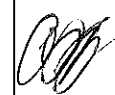
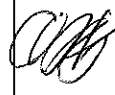
The CA performs the HSM Acceptance Testing by executing the following steps:

- Inspect the HSM's Tamper Evident Bag for tamper evidence
- Set up and configure the testing laptop, peripherals, and connections
- Power on HSM
- Set HSM to secure state
- 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)

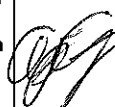
Verify HSM8W Chain of Custody

Step	Activity	Initials	Time
2.1	<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 17). 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 the pre-printed label on the HSM on top of the HSM just over the LCD display.</p> <p>f) Remove the protective film covering the LCD display.</p> <p>g) IW records the battery code of the HSM located on the rear panel.</p> <p>HSM8W Battery Code: <u>23-06</u></p> <p>HSM8W: TEB # 00797152 / Serial # H2110006</p>		17:59
2.2	<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>HSM8W: Serial # H2110006</p> <p>Note: The HSM physical key is used to enable/disable the LCD display and the keypad.</p>		18:01

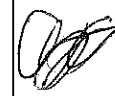
Laptop Setup

Step	Activity	Initials	Time
2.3	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.		18:02
2.4	CA ensures the lock switch on the left side of the listed SD card is slid down to the lock position: OS media release coen-1.0.0		18:02
2.5	CA performs the following steps to boot the testing laptop: a) Connect the null modem cable into a USB port of the laptop. b) Connect the external HDMI display cable. c) Connect the power supply. d) Insert the OS media release coen-1.0.0 . e) Switch it ON.		18:03
2.6	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		18:04


OS Media Checksum Verification

Step	Activity	Initials	Time
2.7	Using the Commands terminal window, CA executes the following steps: a) Verify the byte count of the SD card matches the ISO size by running the following command: <code>df -B1 /dev/sda</code> b) Calculate the SHA-256 hash by executing: <code>head -c 375431168 /dev/sda sha2wordlist</code> c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash. Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script. SHA-256 hash: 405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a PGP Words: crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/52		18:06



Date Setup

Step	Activity	Initials	Time
2.8	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 "20240213 HH:MM:SS"</code> to set the time. where HH is two-digit hour, MM is two-digit minutes and SS is two-digit seconds. b) Execute <code>date</code> to confirm the date/time matches the clock.		18:07


Connect the HSMFD

Step	Activity	Initials	Time
2.9	CA plugs the HSMFD into the USB slot, then performs the steps below: a) Wait for the OS to recognize it. b) Close the file system window.		18:07


Start the Terminal Session Logging

Step	Activity	Initials	Time
2.10	Using the Commands terminal window, CA executes the command below to change the working directory to HSMFD: <code>cd /media/HSMFD</code>		18:07
2.11	CA executes the command below to log activities of the Commands terminal window: <code>script script-20240213.log</code>		18:08


Start the HSM Output Logging

Step	Activity	Initials	Time
2.12	Using the HSM Output terminal window, CA performs the following steps to capture the activity logs of the HSM: a) Change the working directory to HSMFD by executing: <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>ttyaudit /dev/ttyUSB0</code> Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.		18:09


Power ON the HSM8W (Tier 7)

Step	Activity	Initials	Time
2.13	CA performs the following steps to prepare the HSM: 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. Note: Status information should appear in the HSM output terminal window. d) Scroll up on the terminal window while IW verifies the displayed HSM serial number on the screen reads H2110006 . e) IW records the firmware version of the HSM. Firmware Version: <u>3.4</u> f) Scroll down to the end of the terminal window. g) After the completion of the HSM self test the display should say "Important Read Manual" indicating the HSM is in the initialized state. HSM8W: Serial # H2110006 Note: The date and time on the HSM is not used as a reference for logging and timestamp.		18:12


Import the AAK

Step	Activity	Initials	Time
2.14	<p>CA performs the following steps to import the Adapter Authorization Key (AAK):</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "2.Restore AAK", press ENT to confirm. When "Restore AAK?" is displayed, press ENT to confirm. When "Insert Card #X?" is displayed, insert the required AAK card. When "Remove Card?" is displayed, remove the AAK card. Repeat steps d) to e) for the 2nd AAK card. When "Done AAK Imported" is displayed, press ENT to confirm. <p>The cards being used are designated for acceptance testing only. They do not contain production materials. Each card is returned to its designated card holder after use. Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix B number [14].</p>		18:13


Configure the HSM to Secure State

Step	Activity	Initials	Time
2.15	<p>CA performs the following steps to configure the HSM to secure state using Security Officer (SO) cards:</p> <ol style="list-style-type: none"> Utilize the HSM's keyboard to scroll through the menu using < > Select "3.Secure", press ENT to confirm. When "Secure?" is displayed, 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 d) to f) for the 2nd SO card. When "SMK AES Triple DES?" is displayed, press CLR to skip. When "SMK AES" is displayed, press ENT to confirm. When "LAN Port Number?" is displayed, press CLR to skip. When "Enable IPv4/IPv6?" is displayed, press CLR to skip. When "LAN IPv4 Address?" is displayed, press CLR to skip. When "LAN IPv4 Mask?" is displayed, press CLR to skip. When "Set IPv4 Gateway?" is displayed, press CLR to skip. When "LAN IPv6 Address?" is displayed, press CLR to skip. When "LAN IPv6 Mask?" is displayed, press CLR to skip. When "Set IPv6 Gateway?" is displayed, press CLR to skip. When "Remote Mgmt Off Enable?" is displayed, press CLR to skip. When "Remote Mgmt Off" is displayed, press ENT to confirm. When "Change Clock?" is displayed, press CLR to skip. When "Import Config?" is displayed, press CLR to skip. When "FIPS Mode On Disable?" is displayed, press CLR to skip. When "FIPS Mode On" is displayed, press ENT to confirm. When "Global Key Export Enabled" is displayed, press CLR to skip. <p>Done Rebooting Device will be displayed. Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix B number [14].</p>		18:16


Change the API Settings

Step	Activity	Initials	Time
2.16	<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 a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix B number [14].</p>		18:18

Verify the API Settings

Step	Activity	Initials	Time
2.17	<p>CA performs the following steps to dump the status of the HSM:</p> <ul style="list-style-type: none"> a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select "8.HSM Info" from the same menu "Key Mgmt", press ENT to confirm. c) Select "8.Output Info", press ENT to confirm. d) When "Output Info?" is displayed, press ENT to confirm. e) Press CLR twice to return to the main menu "Secured". f) 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. g) After verification, scroll down to the end of the terminal window. <p>Modes: (1=Enabled 0=Disabled)</p> <pre> 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>		18:20

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
2.18	<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 OP card. <p>Confirm the "READY" LED on the HSM is ON.</p> <p>Note: If a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix B number [14].</p>		18:22

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: <u>2</u> Step(s): <u>2.22, 2.23</u> Page(s): <u>12</u> Date and time of the exception: <u>20240213 18:25</u> Note: IW describes the exception(s) and action(s) below.	Ceff	19:03

kSKBackup and kSKGEN were used instead of kskm-keymaster to generate a Temporary key due to the lack of a required configuration file. The command was successful.

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
2.19	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.	<i>CAF</i>	18:22
2.20	CA performs the following steps to test the network connectivity between laptop and HSM: a) Select the Commands terminal window b) Test connectivity by executing: ping hsm c) Wait for responses, then exit by pressing: Ctrl + C	<i>CAF</i>	18:22

Initialize HSM

Step	Activity	Initials	Time
2.21	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"	<i>CAF</i>	18:24

Generate New Test Key

Step	Activity	Initials	Time
2.22	Using the Commands terminal window, the CA executes the command below generate new test key: kskm-keymaster keygen --algorithm RSASHA256 --size 2048	<i>CAF</i>	18:28

Verify the Test KSK

Step	Activity	Initials	Time
2.23	CA checks the Test KSK by executing in to the terminal window: kskm-keymaster inventory Verify the presence of the keypair created previously.	<i>CAF</i>	18:30

Erase / Zeroize / Unsecure HSM8W

Step	Activity	Initials	Time
2.24	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>[Signature]</i>	18:31
2.25	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 a card is unreadable, gently wipe its metal contacts and try again. Use credentials that haven't been used previously during this ceremony when possible. For a summary of card roles and their purpose see Appendix B number [14].</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>[Signature]</i>	18:33
2.26	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.	<i>[Signature]</i>	18:34

Place HSM8W in the TEB

Step	Activity	Initials	Time
2.27	CA performs the following steps to prepare the HSM for storage: <ul style="list-style-type: none"> a) Ask the IW for the HSM's designated new TEB, and read the TEB number aloud while IW verifies it matches the information below. b) Read aloud the HSM serial number while the IW verifies it matches the information below. c) Place the HSM into its designated new TEB and seal it. d) Give IW the sealing strips for post-ceremony inventory. e) Place the HSM onto its designated space on the ceremony table visible to the audit camera. f) Initial the TEB along with IW using a ballpoint pen. g) Place the HSM TEB on the cart. <p>HSM8W: TEB # BB51184549 / Serial # H2110006 ✓</p>	<i>[Signature]</i>	18:36

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

Step	Activity	Initials	Time
2.28	CA places the SO, OP, CO, and AAK cards into a plastic case and hands it to RKOS for use in future acceptance testing ceremonies.	<i>[Signature]</i>	18:36

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
2.29	CA performs the following steps to stop logging: a) Perform the following steps using the HSM Output terminal window to stop logging the serial output (ttyaudit): i) Press Ctrl + C ii) Execute exit b) Execute the command below using the Commands terminal window to stop logging the terminal session: exit Note: The Commands terminal session window will remain open. c) Disconnect the null modem and ethernet cables from the laptop.	CAF	18:37

Copy the HSMFD Contents


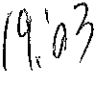
Step	Activity	Initials	Time
2.30	Using the Commands terminal window, CA executes the command below to display the contents of the HSMFD: ls -ltrR	CAF	18:38
2.31	CA executes the command below and follows the interactive prompts in the terminal window to create an HSMFD copy: copy-hsmfd Note: Wait for the activity light on the copied HSMFD to stop flashing before removal.	CAF	18:40

Power OFF the Laptop

Step	Activity	Initials	Time
2.32	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.	CAF	18:41
2.33	CA performs the following steps to shut down the laptop: a) Turn OFF the laptop by pressing the power button. b) Disconnect all connections from the laptop. c) Remove the OS media from the laptop. d) Close all laptop latches.	CAF	18:41

Root DNSSEC Script Exception

Exception Details

Activity	Initials	Time
IW writes the details of the ceremony exception: Act: <u>2</u> Step(s): <u>2,37</u> Page(s): <u>15</u> Date and time of the exception: <u>20240213 18:46</u>		
Note: IW describes the exception(s) and action(s) below.		

The contents of the equipment safe were checked for optimal arrangement and two TEBs, A13004330 and A2751150 containing old new Keyper HSM blank smartcards and old empty TEBs from 2010 were removed as they were not required. The TEBs were opened and inspected. The TEBs were destroyed as were the old Keyper Smartcards.

Open Equipment Safe #1

Step	Activity	Initials	Time
2.34	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)	<i>[Signature]</i>	18:42
2.35	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.	<i>[Signature]</i>	18:44
2.36	Perform the following steps to update the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry then initials it.	<i>[Signature]</i>	18:48
2.37	CA performs the following steps to place the HSM into 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 "Place" is indicated. d) IW verifies the safe log entry, then initials it. HSM8W: TEB # BB51184549 / Serial # H2110006 ✓	<i>[Signature]</i>	18:52

Close Equipment Safe #1

Step	Activity	Initials	Time
2.38	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the entry, then initials it.	<i>[Signature]</i>	18:53
2.39	SSC1 returns the safe log 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 adjacent to the Tier 5 (Safe Room) exit door is off.	<i>[Signature]</i>	18:53
2.40	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	<i>[Signature]</i>	18:54

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
3.1	CA reads all exceptions that occurred during the ceremony.	CAJ	19:03
3.2	CA calls each in-person attendee not seated at the ceremony table to sign the IW's participant list. All signatories declare to the best of their knowledge that this script is a true and accurate record of the ceremony.	CAJ	19:04
3.3	CA reviews IW's script, then signs the participants list.	CAJ	19:05
3.4	IW signs the list and records the completion time.	CAJ	19:05

Stop Recording


Step	Activity	Initials	Time
3.5	CA stops the audit camera video recording.	CAJ	19:01

Appendix A: HSM Chain of Custody

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

[Ext] Chain of Custody - Reference 23JR712335

 Peter Clements (Cyber) <Peter.Clements@ultra-cis.com>
To: andres.pavez@iana.org; aaron.foley@iana.org; Cc: Jasper Rose

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

For the attention of Andres Pavez and Aaron Foley.

Please find details of your order dispatched on 30/06/2023. This email has been signed with a digital signature as requested to confirm chain of custody.

Recipient:

ICANN/IANA
12025 Waterfront Drive
Suite 300
Los Angeles
CA 90094-2536
UNITED STATES

Date	30/06/2023
Customer PO#	23JR712335
Ultra Cyber Ref#	CISD002267
Courier Used	FEDEX INT.
AWB/Tracking #	772610097888
Product Type	AEP-KEY-PLS

Serial Number	Tamper Bag Ref
h2110007	00797151
h2110006	00797152
h2110008	00797153


Upon receipt, please check that the serial number and tamper evident bag are correct. If, with during transit, please contact Ultra.

Peter Clements (He/Him)
Head of Compliance, Cyber UK



View Certificate

- DigiCert Assured ID Root G2
 - DigiCert Assured ID Client CA G2
 - Peter Clements

 **Peter Clements**
Issued by: DigiCert Assured ID Client CA G2
Expires: Tuesday, April 1, 2025 at 16:59:59 Pacific Daylight Time
This certificate is valid

Trust

Details

Subject Name

Country or Region GB
Locality Greenford
Organization Ultra Electronics Limited
Organizational Unit Cyber
Common Name Peter Clements
Email Address peter.clements@ultra-cis.com

Issuer Name

Country or Region US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert Assured ID Client CA G2

Serial Number 0F 16 3A 27 72 FD 36 DB DA 26 AB F2 BF C1 CF FF
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None

?

OK

Appendix B: 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

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 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 21.

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

One set of the audit camera footages.


3. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 52**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

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: Aaron Foley

Signature: 

Date: 2024 Feb 13