Root DNSSEC KSK

Administrative Ceremony
HSM Acceptance Testing

Wednesday 29 November 2023

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	David Huberman / ICANN		2023 Nov 29	17:56
IW	Andy Newton / ICANN			
SSC1	Robert Hoggarth / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
EW	Pia Gruvö			
EW	Nomsa Mwayenga			
EW	Robert Seastrom			
EW	~~Hugo Salgado~~			
EW	Hope Shafer			
EW	James Mitchell			

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

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 1 Step(s): 2 Page(s): 5 Date and Time: 29 Nov 2023 16:20 **Note: IW describes the exception(s) and action(s) below.**	[illegible]	16:20

Hugo Salgado was unable to attend the ceremony.

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.		16:19
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.		16:20
3	CA asks that any first time ceremony participants in the room introduce themselves.		16:21

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.		16:21
5	CA explains the use of personal electronic devices during the ceremony.		16:21
6	CA summarizes the purpose of the ceremony.		16:22

Verify the Time and Date

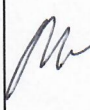
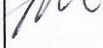
Step	Activity	Initials	Time
7	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: 2023-11-29 16:22 **Note: All entries into this script or any logs should follow this common source of time.**		16:22

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 HSM7E Chain of Custody

Step	Activity	Initials	Time
1	CA performs the following steps to unbox the new HSM. a) Unpack the HSM box while leaving HSM enclosed in the vendor supplied TEB. b) Inspect the HSM vendor supplied TEB for tamper evidence. c) Match HSM serial number and vendor TEB to digitally signed email from the vendor (See Appendix A on page 23). If these do not match, re-package HSMs, terminate the ceremony, and return HSMs. d) Remove and discard the TEB, then place the HSM on its designated area of the ceremony table. e) Affix a label on the HSM. f) IW records the battery code of the HSM located on the rear panel. **HSM7E Battery Code:** 23-06 **HSM7E: TEB # 00797154 / Serial # H2110009**		16:27
2	CA removes the small packet on top of the HSM containing the HSM physical key and performs the following steps: a) Verify the serial number on the packet matches with the HSM serial number. b) Verify the number in the key matches with the number in the packet. c) Return the physical key to the small packet and set it aside for RKOS to store. **HSM7E: Serial # H2110009** **Note: The HSM physical key is used to enable/disable the LCD display and the keypad.**		16:29

Verify HSM8E Chain of Custody

Step	Activity	Initials	Time
3	CA performs the following steps to unbox the new HSM. a) Unpack the HSM box while leaving HSM enclosed in the vendor supplied TEB. b) Inspect the HSM vendor supplied TEB for tamper evidence. c) Match HSM serial number and vendor TEB to digitally signed email from the vendor (See Appendix A on page 23). If these do not match, re-package HSMs, terminate the ceremony, and return HSMs. d) Remove and discard the TEB, then place the HSM on its designated area of the ceremony table. e) Affix a label on the HSM. f) IW records the battery code of the HSM located on the rear panel. **HSM8E Battery Code:** 23-06 **HSM8E: TEB # 00797155 / Serial # H2110010**		16:32
4	CA removes the small packet on top of the HSM containing the HSM physical key and performs the following steps: a) Verify the serial number on the packet matches with the HSM serial number. b) Verify the number in the key matches with the number in the packet. c) Return the physical key to the small packet and set it aside for RKOS to store. **HSM8E: Serial # H2110010** **Note: The HSM physical key is used to enable/disable the LCD display and the keypad.**		16:34

Laptop Setup

Step	Activity	Initials	Time
5	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.		16:34
6	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**		16:35
7	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.		16:36
8	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**		16:37

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 2 Step(s): 13+14 Page(s): 8+9 Date and Time: 29 Nov 2033 16:45 **Note: IW describes the exception(s) and action(s) below.**	AW	16:46

Step 14 was executed in the wrong tab of the terminal program, requiring step 13 and 14 to be re-executed

OS Media Checksum Verification

Step	Activity	Initials	Time

9	CA uses the terminal window to executes the following steps:
	a) Verify the byte count of the SD card matches the ISO size of by running the following command:
	`df -B1 /dev/sda`
	b) Calculate the SHA-256 hash by executing:
	`head -c 375431168 /dev/sda | sha2wordlist`
	c) IW and participants confirm the result matches the PGP Wordlist of the SHA-256 hash.
	Note: CA assigns half of the participants to confirm the hash displayed on the TV screen while the other half confirm the hash from the ceremony script.
	
	SHA-256 hash:
	405d7c76c114feb93fcc5345e13850e59d86341a08161207d8eb8c395410c13a
	PGP Words:
	crackdown filament kiwi impetus snapline belowground woodlark proximate cowbell revolver dwelling detector tempest consulting drumbeat travesty quadrant letterhead choking Bradbury aimless bodyguard atlas amusement stormy underfoot offload corporate eating autopsy snapline corrosion
	
	Note: The SHA-256 hash of the OS media release coen-1.0.0 is also published on the IANA website https://www.iana.org/dnssec/ceremonies/51
		MW	16:39

Date Setup

Step	Activity	Initials	Time
10	CA executes `date` 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 `date -s "20231129 HH:MM:00"` to set the time. **where `HH` is two-digit hour, `MM` is two-digit minutes and `00` is zero seconds.** b) Execute `date` to confirm the date/time matches the clock.	MW	16:40

Connect the HSMFD

Step	Activity	Initials	Time
11	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.	MW	16:41

Start the Terminal Session Logging

Step	Activity	Initials	Time
12	CA executes the command below using the terminal window to change the working directory to HSMFD: `cd /media/HSMFD`	MW	16:41
13	CA executes the command below to log activities of the **Commands** terminal window: `script script-20231129.log`	MW	16:41

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 2 Step(s): 16 Page(s): 9 Date and Time: 29 Nov 2023 16:52 **Note: IW describes the exception(s) and action(s) below.**	[signature]	16:53

In Step 16 part d there is an instruction to press ENT but this was not required by the HSM.

This also applies to Act 2 Step 32 page 15

Start the HSM Output Logging

Step	Activity	Initials	Time

14	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/ttyUSB0 115200`
	c) Start logging the serial output by executing:
	`ttyaudit /dev/ttyUSB0`
	Note: DO NOT unplug the null modem cable from the laptop as this will stop capturing activity logs from the HSM.
		AW	16:42

Power ON the HSM7E (Tier 7)

Step	Activity	Initials	Time
15	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 logging screen.** 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 **H2110009**. f) IW records the firmware version of the HSM. **Firmware Version:** 3.4 g) Scroll down to the end of the logging screen. h) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **HSM7E: Serial # H2110009** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	AW	16:49

Import the AAK

Step	Activity	Initials	Time
16	CA performs the following steps to import the Adapter Authorization Key (AAK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Restore AAK"**, press **ENT** to confirm. c) When **"Restore AAK?"** is displayed, press **ENT** to confirm. d) When **"Insert Card #X?"** is displayed, insert the required AAK card and press **ENT**. e) When **"Remove Card?"** is displayed, remove the AAK card. f) Repeat steps d) to e) for the 2nd AAK card. g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm. 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.** **For a summary of card roles and their purpose see Appendix B number [14].**	AW	16:52

Configure the HSM to Secure State

Step	Activity	Initials	Time
17	CA performs the following steps to configure the HSM to secure state using Security Officer (SO) cards: 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. **Done Rebooting Device** will be displayed. **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].**	MV	1615Z

Change the API Settings

Step	Activity	Initials	Time
18	CA performs the following steps to change the API settings: 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"** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].**	AW	16:58

Verify the API Settings

Step	Activity	Initials	Time

19	CA performs the following steps to dump the status of the HSM:
	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"**
	
	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:
	
	`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`
		AV	17:01

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
20	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert 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. Confirm the **"READY"** LED on the **HSM** is **ON.** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].**	AV	17:02

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
21	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		17:03

22	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`
			17:03

Initialize HSM

Step	Activity	Initials	Time

23	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"
			17:04

Generate New Test Key

Step	Activity	Initials	Time
24	CA executes the command below in the terminal window to generate new test key: `kskm-keymaster keygen --algorithm RSASHA256 --size 2048`		17:04

Verify the Test KSK

Step	Activity	Initials	Time
25	CA checks the Test KSK by executing in to the terminal window: `kskm-keymaster inventory` Verify the presence of the keypair created previously.		17:05

Erase / Zeroize / Unsecure HSM7E

Step	Activity	Initials	Time
26	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**.		17:06
27	CA performs the following steps to return the HSM to **Unsecure** factory default state. This will erase all keys, settings, and configuration. 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**. **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].** It may take a few minutes for the HSM to restart after the zeroization is complete. 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.		17:08
28	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.		17:09

Place HSM7E in the TEB

Step	Activity	Initials	Time
29	CA places the HSM into its designated new TEB, then seals it.		17:11
30	CA performs the following steps to verify the TEB: 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. **HSM7E: TEB # BB51184253 / Serial # H2110009**		17:12

Power ON the HSM8E (Tier 7)

Step	Activity	Initials	Time
31	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 logging screen.** 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 **H2110010**. f) IW records the firmware version of the HSM. **Firmware Version:** 3.4 g) Scroll down to the end of the logging screen. h) After the completion of the HSM self test the display should say **"Important Read Manual"** indicating the HSM is in the initialized state. **HSM8E: Serial # H2110010** **Note: The date and time on the HSM is not used as a reference for logging and timestamp.**	AN	17:15

Import the AAK

Step	Activity	Initials	Time
32	CA performs the following steps to import the Adapter Authorization Key (AAK): a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"2.Restore AAK"**, press **ENT** to confirm. c) When **"Restore AAK?"** is displayed, press **ENT** to confirm. d) When **"Insert Card #X?"** is displayed, insert the required AAK card and press **ENT**. e) When **"Remove Card?"** is displayed, remove the AAK card. f) Repeat steps d) to e) for the 2nd AAK card. g) When **"Done AAK Imported"** is displayed, press **ENT** to confirm. 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.** **For a summary of card roles and their purpose see Appendix B number [14].**	AN	17:16

Configure the HSM to Secure State

Step	Activity	Initials	Time
33	CA performs the following steps to configure the HSM to secure state using Security Officer (SO) cards: 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. **Done Rebooting Device** will be displayed. **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].**	AW	17:19

Change the API Settings

Step	Activity	Initials	Time
34	CA performs the following steps to change the API settings: 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"** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].**	AR	17:21

Verify the API Settings

Step	Activity	Initials	Time

35	CA performs the following steps to dump the status of the HSM:
	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"**
	
	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:
	
	`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`
		IW	17:22

Enable/Activate the HSM (Tier 7)

Step	Activity	Initials	Time
36	CA performs the following steps to activate the HSM: a) Utilize the HSM's keyboard to scroll through the menu using < > b) Select **"1.Set Online"**, press **ENT** to confirm. c) When **"Set Online?"** is displayed, press **ENT** to confirm. d) When **"Insert Card OP #X?"** is displayed, insert 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. Confirm the **"READY"** LED on the **HSM** is **ON.** **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].**	IW	17:23

Check the Network Connectivity Between Laptop and HSM

Step	Activity	Initials	Time
37	CA connects the HSM to the laptop using an ethernet cable in the LAN ports.		17:24

38	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`
			17:25

Generate New Test Key

Step	Activity	Initials	Time
39	CA executes the command below in the terminal window to generate new test key: `kskm-keymaster keygen --algorithm RSASHA256 --size 2048`		17:26

Verify the Test KSK

Step	Activity	Initials	Time
40	CA checks the Test KSK by executing in to the terminal window: `kskm-keymaster inventory` Verify the presence of the keypair created previously.		17:26

Erase / Zeroize / Unsecure HSM8E

Step	Activity	Initials	Time
41	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**.		17:27
42	CA performs the following steps to return the HSM to **Unsecure** factory default state. This will erase all keys, settings, and configuration. 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**. **Note: If a card is unreadable, gently wipe its metal contacts and try again.** **For a summary of card roles and their purpose see Appendix B number [14].** It may take a few minutes for the HSM to restart after the zeroization is complete. 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.		17:28
43	CA switches the HSM power to OFF, then disconnects the power, serial, and ethernet connections.		17:29

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 2 Step(s): 49 Page(s): ~~50~~ Date and Time: 29 Nov 2023 17:38 **Note: IW describes the exception(s) and action(s) below.**	M	17:39

In following the copy, the script did not contain the necessary subsequent steps for inserting a second OBB stick and copying. The script should instruct the CA to follow the prompts on the screen.

Place HSM8E in the TEB

Step	Activity	Initials	Time
44	CA places the HSM into its designated new TEB, then seals it.		17:29
45	CA performs the following steps to verify the TEB: 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. **HSM8E: TEB # BB51184254 / Serial # H2110010**		17:31

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

Step	Activity	Initials	Time
46	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.		17:32

Stop logging the Serial Output and the Terminal Session

Step	Activity	Initials	Time
47	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.		17:32

Copy the HSMFD Contents

Step	Activity	Initials	Time
48	CA executes the command below using the terminal window to display the contents of the HSMFD: `ls -ltrR`		17:33
49	CA executes the command below to create an HSMFD copy: `copy-hsmfd` **Note: Wait for the activity light on the copy HSMFD to stop flashing before removal.**		17:33

Power OFF the Laptop

Step	Activity	Initials	Time
50	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.		17:40
51	CA performs the following steps to switch OFF the laptop and remove the OS media: 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.		17:41

Open Equipment Safe #1

Step	Activity	Initials	Time
52	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		17:43
53	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.**		17:45
54	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.		17:46
55	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. **HSM7E: TEB # BB51184253 / Serial # H2110009** **HSM8E: TEB # BB51184254 / Serial # H2110010**		17:48

Close Equipment Safe #1

Step	Activity	Initials	Time
56	SSC1 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the entry, then initials it.		17:49
57	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 is off.		17:50
58	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		17:51

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.		17:52
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.**		17:54
3	CA reviews IW's script, then signs the participants list.		17:55
4	IW signs the list and records the completion time.		17:56

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

Step	Activity	Initials	Time
5	CA stops the audit camera video recording.		17:56
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).		18:00

Bundle Audit Materials

Step	Activity	Initials	Time
7	IW makes a copy of their script for off-site audit bundle containing: a) Copy of IW's administrative ceremony script. b) Audio-visual recording. c) IW's attestation (See Appendix D on page 27). 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.		19:30

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
18155 Technology Drive
Virginia
Culpeper
VA 22701
UNITED STATES

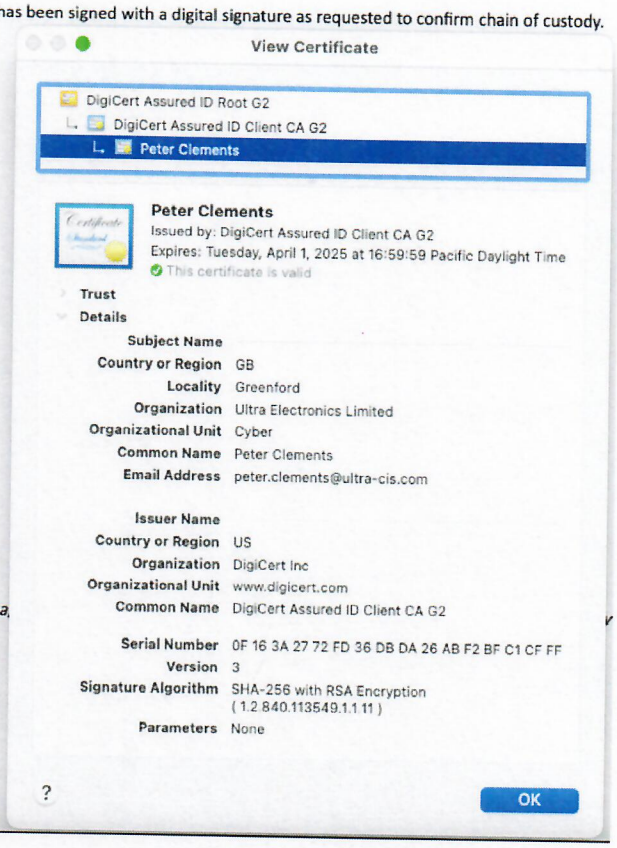
Date	30/06/2023
Customer PO#	23JR712335
Ultra Cyber Ref#	CISD002268
Courier Used	FEDEX INT.
AWB/Tracking #	772610172810
Product Type	AEP-KEY-PLS

Serial Number	Tamper Bag Ref
h2110009	00797154
h2110010	00797155
h2110011	00797156

Upon receipt, please check that the serial number and tamper evident ba
with during transit, please contact Ultra.

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

ULTRA | Intelligence & Communications
DIVERSE. INCLUSIVE. ACCEPTING. WELCOMING. SAFE SPACE. FOR EVERYONE.



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 27.

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: _____

Signature: Andrew Newton

Date: 2023 Nov 29