Root DNSSEC KSK

Administrative Ceremony
Safe #1 Equipment Maintenance

Thursday 10 June 2021

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

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	Andres Pavez / PTI	*[signature]*		
IW	Aaron Foley / PTI	*[signature]*		
SSC1_A	Paul Hoffman / ICANN	*[signature]*	2021 Jun 10	14:3
SSC1_B	Fernanda Iunes / ICANN	*[signature]*		

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.	*(initials)*	14:01
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.	*(initials)*	14:01
3	CA asks that any first time ceremony participants in the room introduce themselves.	*(initials)*	14:02

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.	*(initials)*	14:02
5	CA explains the use of personal electronic devices during the ceremony.	*(initials)*	14:03
6	CA summarizes the purpose of the ceremony.	*(initials)*	14:03

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: 2021-06-10 14:03 Note: All entries into this script or any logs should follow this common source of time.	*(initials)*	14:03

Act 2: Safe #1 Equipment Maintenance

The CA will oversee the safe maintenance by executing the following steps:

- Escort required personnel to Tier 5 (Safe Room).
- SSC1_A will open the safe.
- SSC1_A will program the new safe dial lock mechanism combination.
- Proper operation of the safe is verified, and required personnel will return to Tier 4 (Ceremony Room).

Open Equipment Safe #1

Step	Activity	Initials	Time
1	CA and IW transport a flashlight, phillips screwdriver, change key tool and escort required personnel into Tier 5 (Safe Room.)	*(initialed)*	14:04
2	SSC1_A 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.**	*(initialed)*	14:07
3	Complete the safe log by following the steps below: a) SSC1_A 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_A. c) SSC1_A writes the date and time, then signs the safe log where **"Open Safe"** is indicated. d) IW verifies this entry then initials it.	*(initialed)*	14:08

Set New Combination for Equipment Safe #1

Step	Activity	Initials	Time
4	CA and SSC1_A prepare for the safe combination change by performing the following steps: **Note: If the access plate on the safe door has already been removed, skip the steps a) and b).** a) Locate the rectangular plate secured to the interior side of the safe door and remove the screws securing it using a phillips screwdriver. b) Slide out the 3-1/2 x 12 inch steel plate covering the interior side of the combination dial. c) Insert the change key tool in the interior side of the combination dial. d) Press the button located at the interior side upper left corner of the safe door to release the bolt.	*(initials)*	14:10
5	SSC1_A initiates the combination change by performing the following steps: a) Charge the dial by rapidly spinning the dial counter-clockwise until numbers are displayed. **Note: A key symbol is displayed, which indicates "Change Key" mode.** b) Continue spinning the dial counter-clockwise to the first number of the combination, then stop at the selected number. c) Spin the dial clockwise to the second number of the combination, then stop at the selected number. d) Spin the dial counter-clockwise to the last number of the combination, then stop at the selected number. e) Spin the dial clockwise until you see the symbol **"SL"** (Select Mode) is displayed. **Note: Repeat steps a) to e) if the symbol "SL" did not display.** f) Turn the dial counter-clockwise, then stop at number **"01"** to select Single Combination Mode operation g) Turn dial clockwise until the symbol **"EC"** (Enter Combination) is displayed. **Note: Immediately perform succeeding steps to avoid timeout**	*(initials)*	14:17
6	SSC1_A programs the **NEW combination** by following the steps below: a) Spin the dial counter-clockwise to the first number of the combination, then stop at the selected number. b) Spin the dial clockwise to the second number of the combination, then stop at the selected number. c) Spin the dial counter-clockwise to the last number of the combination, then stop at the selected number. **Note: Repeat step 5 if any errors occur.** d) Spin the dial clockwise for the display to cycle through the new combination. SSC1_A should verify the new combination. e) Remove the Change Key tool when **"PO"** (Pull Out Change Key) is displayed. The Change Key symbol will disappear and **"CC"** (Confirm Combination) will appear. f) Enter the **NEW combination** once again for confirmation. g) Spin the dial clockwise after **"OP"** with a right arrow (OPen right) is displayed, continue dialing to the clockwise to retract the lock bolt. The new combination is now set.	*(initials)*	14:17

Verify New Combination and Close the Equipment Safe #1

Step	Activity	Initials	Time
7	SSC1_A performs the following steps: a) Return the Change Key tool to IW b) Reinstall the cover plate to the safe door. c) Return the screwdriver to IW **Note: DO NOT close the Safe door.**	*(initials)*	14:19
8	SSC1_A and SSC1_B performs additional tests on the dial if necessary. **Note: DO NOT Close the Safe door.**	*(initials)*	14:22
9	SSC1_A writes the date and time, then signs the safe log where **"Change Combination"** and **"Close Safe"** are indicated. IW verifies the safe log entries, then initials it.	*(initials)*	14:24
10	SSC1_A returns the safe log inside Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	*(initials)*	14:24

Test the Equipment Safe #1 and Exit the Safe Room

Step	Activity	Initials	Time
11	SSC1_A 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.**	*(initials)*	14:26
12	SSC1_A removes the existing safe log, writes the date and time, then signs the safe log where **"Open Safe"** and **"Close Safe"** is indicated. IW verifies this entry then initials it.	*(initials)*	14:27
13	SSC1_A returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the **"WAIT"** light indicator is off.	*(initials)*	14:27
14	SSC1_B repeats the steps 11 to 13.	*(initials)*	14:29
15	CA, IW, and any escorted personnel leave Tier 5 (Safe Room), returning to Tier 4 (Key Ceremony Room).	*(initials)*	14:30

Act 3: Close the Administrative Ceremony

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

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

Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.	*[signature]*	14:30
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.**	*[signature]*	14:31
3	CA reviews IW's script, then signs the participants list.	*[signature]*	14:32
4	IW signs the list and records the completion time.	*[signature]*	14:32

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

Step	Activity	Initials	Time
5	CA stops the audit camera video recording.	*[signature]*	14:34
6	CA and IW ensures that all participants are signed out of Tier 4 (Key Ceremony Room) log and escorted out of Tier 4 (Key Ceremony Room.)	*[signature]*	14:35

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 B on page 11). All TEBs are labeled **Root DNSSEC Administrative Ceremony Safe #1 Equipment Maintenance**, dated and signed by IW and CA. An off-site audit bundle is delivered to an off-site storage.	*[signature]*	15:35

Appendix A: Audit Bundle Checklist

1. Administrative Ceremony Script (by IW)

Hard copies of the IW's administrative ceremony script, including notes and attestation. See Appendix B on page 11.

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

One set for the audit bundle.

3. Other items

If applicable.

Appendix B: 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: 2021 Jun 10