

**Root DNSSEC KSK**  
Administrative Ceremony  
Safe #1 Equipment Functionality

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)

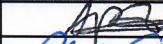


## Abbreviations

<b>AUD</b> = Third Party Auditor	<b>CA</b> = Ceremony Administrator	<b>CO</b> = Crypto Officer
<b>EW</b> = External Witness	<b>FD</b> = Flash Drive	<b>HSM</b> = Hardware Security Module
<b>IW</b> = Internal Witness	<b>KMF</b> = Key Management Facility	<b>KSR</b> = Key Signing Request
<b>OP</b> = Operator	<b>PTI</b> = Public Technical Identifiers	<b>RKSH</b> = Recovery Key Share Holder
<b>RKOS</b> = RZ KSK Operations Security	<b>RZM</b> = Root Zone Maintainer	<b>SA</b> = System Administrator
<b>SKR</b> = Signed Key Response	<b>SMK</b> = Storage Master Key	<b>SO</b> = Security Officer
<b>SSC</b> = Safe Security Controller	<b>SW</b> = Staff Witness	<b>TCR</b> = Trusted Community Representative
<b>TEB</b> = 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		2021 Jun 10	15:32
IW	Aaron Foley / PTI			
SSC1	Paul Hoffman / ICANN			

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

## Instructions for a Root DNSSEC KSK Administrative Ceremony

The Root DNSSEC Key Signing Key (KSK) Administrative Ceremony is a scripted meeting where individuals with specific roles perform tasks related to support the operation of the root zone KSK. Administrative Ceremonies include all ceremonies that do not require use of the private key component of the root zone DNSSEC KSK, such as enrollment or replacement of a trusted role, media deposit or extraction, equipment acceptance testing or maintenance, etc. The process is audited by a third party firm for compliance with SOC 3 framework. The script and recordings are published online for the wider Internet community to review.

### Ceremony Guidelines:

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

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

### Key Management Facility Tiers:

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

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

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

## Act 1: Initiate Ceremony

The CA initiates the ceremony by performing the steps below:

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

### Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1	CA confirms that required audit cameras are recording.	<i>[Signature]</i>	15:02
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>	15:02
3	CA asks that any first time ceremony participants in the room introduce themselves.	<i>[Signature]</i>	15:02

### Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.	<i>[Signature]</i>	15:03
5	CA explains the use of personal electronic devices during the ceremony.	<i>[Signature]</i>	15:03
6	CA summarizes the purpose of the ceremony.	<i>[Signature]</i>	15:04

### Verify the Time and Date

Step	Activity	Initials	Time
7	IW enters UTC date (YYYY-MM-DD) and time (HH:MM) using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: <u>2021-06-10 15:04</u>	<i>[Signature]</i>	15:04
Note: All entries into this script or any logs should follow this common source of time.			

## Act 2: Safe #1 Equipment Functionality

The CA tests the functionality of the Hardware Security Modules (HSMs) by executing the following steps:

### Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
1	CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)	<i>[Signature]</i>	15:05
2	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>	15:06
3	Perform the following steps to complete the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.	<i>[Signature]</i>	15:08



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

Step	Activity	Initials	Time
4	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified in the list below. d) Write the date, time, and signature on the safe log where "Remove" is indicated. e) IW verifies the safe log entry, then initials it.  HSM4: TEB # BB51184226 (Place on Cart) Last Verified: KSK39 2019-11-14 HSM5E: TEB # BB51184524 (Place on Cart) Last Verified: KSK37 2019-05-16  Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.	<i>[Signature]</i>	15:10

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

Step	Activity	Initials	Time
5	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the safe log entry then initials it.	<i>[Signature]</i>	15:11
6	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.	<i>[Signature]</i>	15:11
7	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).	<i>[Signature]</i>	15:12

## Power on (without activation) HSMs (Tier 7) to ensure no tamper indication

Step	Activity	Initials	Time
8	<p>CA performs the following steps to prepare the equipment for testing:</p> <ol style="list-style-type: none"> <li>Remove all equipment TEBs from the cart and place them on the ceremony table.</li> <li>Inspect each equipment TEB for tamper evidence.</li> <li>Read aloud the TEB number and the serial number (if applicable) while IW verifies the information using the previous ceremony script where it was last used.</li> <li>Remove and discard the TEB, then place the equipment on the ceremony table.</li> </ol> <p><b>HSM4: TEB # BB51184226 / Serial # H1411011</b>  <i>Last Verified: KSK39 2019-11-14</i>  <b>HSM5E: TEB # BB51184524 / Serial # H1903018</b>  <i>Last Verified: KSK37 2019-05-16</i></p> <p><small>Note: "Last verified" indicates the last time a piece of equipment was placed in a new TEB during a ceremony. It is listed here for audit tracking purposes.</small></p>		<p>15:15</p>
9	<p>CA performs the following steps to test HSMs for tamper indication and check battery status:</p> <ol style="list-style-type: none"> <li>Place the first available HSM listed below in the designated HSM area on the ceremony table.</li> <li>Ensure an RJ45 blockout is present in the "MGMT" port of the HSM. Install one if not present.</li> <li>Connect the power to the HSM.</li> <li>Activate the rocker switch on the back of the HSM to power it on.</li> <li>The power light will activate and self testing will commence. Ensure that "Secured" appears in the upper left portion of the HSM's display and the alert light is not activated which would indicate a tamper.</li> <li>IW records the HSM tamper indication below.</li> <li>If there is a tamper indication, continue with the step m). If not, perform the following steps to check the HSM battery status:</li> <li>Utilize the HSM's keyboard to scroll through the menu using &lt; &gt;</li> <li>Select "4.HSM Info", press <b>ENT</b> to confirm.</li> <li>Select "1.Battery Status", press <b>ENT</b> to confirm.</li> <li>IW records the HSM battery status below.</li> <li>Press <b>CLR twice</b> to return to the main menu "Secured".</li> <li>Switch the HSM off and set it aside to be placed into a TEB.</li> <li>Repeat steps a) to m) for the remaining HSMs listed below.</li> </ol> <p>HSM4 Tamper: <u>none</u> Battery: <u>ok</u>  HSM5E Tamper: <u>none</u> Battery: <u>ok</u></p>		<p>15:21</p>

### Place the HSMs (Tier 7) into a TEB

Step	Activity	Initials	Time
10	<p>CA performs the following steps:</p> <p>a) Place the first available HSM listed below into a TEB</p> <p>b) Read aloud the TEB number and HSM serial number, then show it to the audit camera above for participants to see.</p> <p>c) Confirm with IW that the TEB number and HSM serial number match below.</p> <p>d) Initial the TEB along with IW using a ballpoint pen.</p> <p>e) Give IW the sealing strips for post-ceremony inventory.</p> <p>f) Place the HSM TEB on the cart.</p> <p>g) Repeat steps a) to f) for the remaining HSMs listed below.</p> <p><b>HSM4: TEB # BB51184675 / Serial # H1411011</b>  <b>HSM5E: TEB # BB51184674 / Serial # H1903018</b></p>		15:25

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

Step	Activity	Initials	Time
11	CA and IW transport a cart and escort SSC1 into Tier 5 (Safe Room.)		15:26
12	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.		15:27
13	SSC1 removes the safe log, then writes the date and time, then signs the safe log where "Open Safe" is indicated. IW verifies this entry, then initials it. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.		15:28
14	<p>CA performs the following steps to return each piece of equipment to the safe:</p> <p>a) CAREFULLY remove the equipment TEB from the cart.</p> <p>b) Read aloud the TEB number while showing it to the audit camera above, then place it inside Safe #1</p> <p>c) Write the date, time, and signature on the safe log where "Return" is indicated.</p> <p>d) IW verifies the safe log entry, then initials it.</p> <p><b>HSM4: TEB # BB51184675</b>  <b>HSM5E: TEB # BB51184674</b></p>		15:29

### Close Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
15	SSC1 writes the date and time, then signs the safe log where "Close Safe" is indicated. IW verifies the entry, then initials it.		15:29
16	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.		15:30
17	CA, SSC1, and IW leave Tier 5 (Safe Room) transporting the cart and returning to Tier 4 (Key Ceremony Room).		15:30



## 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.	<i>CA</i>	15:31
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. <b>All signatories declare that this script is a true and accurate record of the ceremony.</b>	<i>CA</i>	15:32
3	CA reviews IW's script, then signs the participants list.	<i>CA</i>	15:32
4	IW signs the list and records the completion time.	<i>IW</i>	15:32

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

Step	Activity	Initials	Time
5	CA stops the audit camera video recording.	<i>CA</i>	15:35
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.)	<i>CA</i>	15:35

### Bundle Audit Materials

Step	Activity	Initials	Time
7	<p>IW makes a copy of their script for off-site audit bundle containing:</p> <ul style="list-style-type: none"> <li>a) Copy of IW's administrative ceremony script.</li> <li>b) Audio-visual recording.</li> <li>c) IW's attestation (See Appendix B on page 11).</li> </ul> <p>All TEBs are labeled <b>Root DNSSEC Administrative Ceremony Safe #1 Equipment Functionality</b>, dated and signed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>	<i>CA</i>	16:02

## **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