

**Root DNSSEC KSK**  
Administrative Ceremony  
Safe Deposit Box Lock Assembly Programming

Monday February 10, 2020

Root Zone KSK Operator Key Management Facility  
1920 East Maple Avenue, El Segundo, CA 90245

This ceremony is executed in accordance to the DNSSEC Practice Statement for the Root Zone KSK Operator Version 4th Edition (2016-10-01)




## 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		2020 Feb 10	22:30
IW	Aaron Foley / PTI			
Locksmith	Richard Bowen / Industrial Lock and Security			

**Note: 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 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 CAs, IWs, or SAs 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
- CAs, IWs, or SAs may escort participants out of Tier 4 (Key Ceremony Room) at the CA's discretion only if Tier 5 (Safe Room) is not occupied during the ceremony
- All participants are required to sign in and out of Tier 4 (Key Ceremony Room) using the visitor log
- The SA starts filming before the participants enter Tier 4 (Key Ceremony Room)
- Ceremony participants follow the script step by step
- CA reads each step aloud prior to its performance
- Upon completion of each step, IW announces the time of completion, records the completion time, and initials their copy of the script
- Ceremony participants who notice a problem or an error during the ceremony should interrupt the ceremony. Ceremony participants agree on a resolution before proceeding
- 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 tell and/or confirm identifiers comprised of numbers and letters. When spelling identifiers, the phonetic alphabet shown below must 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

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

Step	Activity	Initials	Time
1	CA confirms that required audit cameras are recording.	[Signature]	20:16
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.	[Signature]	20:17

### Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3	CA reviews emergency evacuation procedures with onsite participants.	[Signature]	20:17
4	CA explains the use of personal electronic devices during the ceremony.	[Signature]	20:18
5	CA briefly explains the purpose of the ceremony.	[Signature]	20:18

### Verify the Time and Date

Step	Activity	Initials	Time
6	IW enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in Tier 4 (Key Ceremony Room): Date and time: <u>2020/02/10 20:18:45</u>	[Signature]	20:18
Note: All entries into this script or any logs should follow this common source of time.			

## Act 2: Safe Deposit Box Lock Assembly Programming

### Preparation

Step	Activity	Initials	Time
1	CA and IW escort the locksmith to the facility mail room to retrieve new safe deposit box lock assemblies, then return to Tier 4 (Ceremony Room).	<i>[Signature]</i>	20:27
2	The locksmith along with CA and IW will remove safe deposit box lock assemblies from the packaging in which they shipped and ensure they are the correct model.	<i>[Signature]</i>	20:32
3	The locksmith along with CA and IW will separate the safe deposit box lock assemblies into two groups of twenty, designated for the two different key management facilities.	<i>[Signature]</i>	20:32

### Safe Deposit Box Lock Programming


Note: tenant keys will remain inserted in their respective locks upon completion of testing.

Note: The guard keys and copies were created previously at the locksmith's facility, observed by CA and IW, and remained in CA and IW custody.

Step	Activity	Initials	Time
4	The locksmith along with CA and IW will program and test each individual safe deposit box lock assembly in the first group of twenty safe deposit box lock assemblies with the pre-programmed <b>guard key west</b> , ensuring functionality for both the guard key and copies, as well as the supplied tenant keys and copies.	<i>[Signature]</i>	21:19
5	The locksmith along with CA and IW will program and test each individual safe deposit box lock assembly in the second group of twenty safe deposit box lock assemblies with the pre-programmed <b>guard key east</b> , ensuring functionality for both the guard key and copies, as well as the supplied tenant keys and copies.	<i>[Signature]</i>	21:46

## Root DNSSEC Script Exception

### Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: <u>2</u> Step(s): <u>10</u> Page(s): <u>7</u> Date and Time: <u>22:07</u>		<u>22:51</u>
2.	IW describes the exception(s) and action(s) below.		

The last KMF West Lock Assembly was malfunctioning, and we delayed the bagging of the unit to allow more time for the locksmith to troubleshoot. Once the lock assembly was functioning, we placed it in TEB BB91951419 and continued where we left off in the script

## KMF West Safe Deposit Box Lock Assembly Packaging

Step	Activity	Initials	Time
6	CA places five safe deposit box lock assemblies programmed with <b>guard key west</b> into TEB # <b>BB46584430</b> , reads aloud the TEB number and description, then seals it.	<i>[Signature]</i>	21:50
7	IW inspects the TEB, confirms the TEB number, then initials it with a ballpoint pen.	<i>[Signature]</i>	21:50
8	CA places one safe deposit box lock assembly programmed with <b>guard key west</b> into the first available empty TEB listed in step 10, reads aloud the TEB number and description, then seals it.	<i>[Signature]</i>	21:52
9	IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.	<i>[Signature]</i>	21:53
10	CA and IW repeat steps 8 to 9 until all safe deposit box lock assemblies programmed with <b>guard key west</b> are stored in TEBs. BB46584433 ✓ BB46584434 ✓ BB91951431 ✓ BB91951430 ✓ BB91951429 ✓ BB91951428 ✓ BB91951427 ✓ BB91951426 ✓ BB91951425 ✓ BB91951424 ✓ BB91951423 ✓ BB91951422 ✓ BB91951421 ✓ BB91951420 ✓ BB91951419 — ? Exception	<i>[Signature]</i>	22:07 22:25
11	CA places all TEBs containing safe deposit box lock assemblies programmed with <b>guard key west</b> onto the equipment cart, then along with IW and locksmith, places the cart in Tier 5 (Safe Room).	<i>[Signature]</i>	22:26



## KMF East Safe Deposit Box Lock Assembly Packaging

Step	Activity	Initials	Time
12	CA places five safe deposit box lock assemblies programmed with <b>guard key east</b> into TEB # <b>BB46584431</b> , reads aloud the TEB number and description, then seals it.	<i>[Signature]</i>	22:09
13	IW inspects the TEB, confirms the TEB number, then initials it with a ballpoint pen.	<i>[Signature]</i>	22:10
14	CA places one safe deposit box lock assembly programmed with <b>guard key east</b> into the first available empty TEB listed in step 16, reads aloud the TEB number and description, then seals it.	<i>[Signature]</i>	22:11
15	IW inspects the TEB, confirms the TEB number with the list below, then initials it with a ballpoint pen.	<i>[Signature]</i>	22:11
16	CA and IW repeat steps 14 to 15 until all safe deposit box lock assemblies programmed with <b>guard key east</b> are stored in TEBs. BB91951418 ✓ BB91951417 ✓ BB91951416 ✓ BB91951415 ✓ BB91951414 ✓ BB91951413 ✓ BB91951412 ✓ BB91951411 ✓ BB91951410 ✓ BB91951409 ✓ BB91951408 ✓ BB91951407 ✓ BB91951406 ✓ BB91951405 ✓ BB91951401 ✓	<i>[Signature]</i>	22:23
17	CA places all TEBs containing safe deposit box lock assemblies programmed with <b>guard key east</b> into a large box pending transportation to KMF East.	<i>[Signature]</i>	22:28

## Act 3: Close the Administrative Ceremony

### Participants Sign IW's Script

Step	Activity	Initials	Time
1	CA reads all exceptions that occurred during the ceremony.	<i>[Signature]</i>	22:29
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. <b>All signatures declare that this script is a true and accurate record of the ceremony.</b>	<i>[Signature]</i>	22:30
3	CA reviews IW's script, then signs the participants list.	<i>[Signature]</i>	22:31
4	IW signs the list and records the completion time.	<i>[Signature]</i>	22:31

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

Step	Activity	Initials	Time
5	CA stops the audit camera video recording.	<i>[Signature]</i>	22:32
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>[Signature]</i>	22:54

### 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 (Appendix B).</li> </ul> <p>All TEBs are labeled <b>Root DNSSEC Administrative Ceremony Safe Deposit Box Lock Assembly Programming</b>, dated and signed by IW and CA. An off-site audit bundle is delivered to an off-site storage.</p>	<i>[Signature]</i>	22:54

## **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.

### **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: 2020 Feb 10