Root DNSSEC KSK

Administrative Ceremony
Safe #2 Credentials Maintenance

Tuesday February 11, 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

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		2020 Feb 12	3'20
IW	Aaron Foley / PTI			
IW_Backup	Jonathan Denison / ICANN			
SSC2	Hilary Jin / ICANN			
Locksmith	Richard Bowen / Industrial Lock and Security			
SA	Brian Martin / ICANN			
EW	Subramanian Moonesamy			
EW	Arbogast Fabian			

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 with SA that audit cameras **1** and **3** are recording. **Note: Audit camera 2 is not recording because there are no production materials placed on the ceremony table.**		1:01
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.		1:01

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3	CA reviews emergency evacuation procedures with onsite participants.		1:02
4	CA explains the use of personal electronic devices during the ceremony.		1:02
5	CA briefly explains the purpose of the ceremony.		1:03

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: ~~2020~~ 2020/02/12 1:04 **Note: All entries into this script or any logs should follow this common source of time.**		1:05

Act 2: Safe #2 Credentials Maintenance

Open Credentials Safe #2

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.)		1:06
2	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.**		1:08
3	Complete the safe log by following the steps below: a) SSC2 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC2. c) SSC2 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies this entry then initials it.		1:09

Replace Combination Lock on Credentials Safe #2

Step	Activity	Initials	Time
4	The locksmith performs the following tasks to replace the combination lock: a) Remove the current Kaba Mas X-09. b) Install a new Kaba Mas X-10. **Note: CA and IW will provide assistance to the locksmith if necessary. The new lock is preconfigured with Single Combination Mode and default combination of 50-25-50.**		2:17

Set New Combination for Credentials Safe #2

Step	Activity	Initials	Time
5	CA and SSC2 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.		2:19
6	SSC2 enters the **CURRENT combination** 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**		2:23
7	SSC2 enters 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 6 if any errors occur.** d) Spin the dial clockwise for the display to cycle through the new combination. SSC2 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.		2:28

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 2 Step(s): 10 Page(s): 8 Date and Time: 20200212 2:55	[illegible]	2:55
2.	IW describes the exception(s) and action(s) below.	[illegible]	2:55

One of the five designated lock assemblies was malfunctioning. One additional lock assembly was used from TEB BB91951419

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1.	IW writes the details of the ceremony exception: Act: 2 Step(s): 12 Page(s): 8 Date and Time: 20200212 3:00	[illegible]	3:00
2.	IW describes the exception(s) and action(s) below.	[illegible]	3:00

The safe did not have enough space to hold the lock assemblies. It was decided to keep them in TEBs in Tier 4 going forward instead.

Replace Safe Deposit Box Lock Assemblies

Step	Activity	Initials	Time
8	CA removes TEB #**BB46584430** from the equipment cart, reads aloud the TEB #, and along with IW inspects it for tamper evidence.		2:29
9	CA opens TEB #**BB46584430** and places its contents on top of Safe 2 (Credentials Safe) for the Locksmith to use.		2:31
10	Locksmith replaces safe deposit box lock assemblies by performing the following steps: a) After the CA operates the guard key in the bottom lock, the locksmith opens the first safe deposit box listed below. b) Locksmith removes the current safe deposit box lock assembly. c) Locksmith installs a new safe deposit box lock assembly. d) After the CA operates the guard key in the bottom lock, the locksmith closes the first safe deposit box listed below, leaving the tenant keys installed in the lock. e) CA applies a **red** circular sticker to the door of the safe deposit box to denote the corresponding guard key. f) Repeat steps a) to e) to replace the safe deposit box lock assemblies for each of the remaining safe deposit boxes listed below. **Box # 1788** **Box # 1790** **Box # 1069** **Box # 1070** **Box # 1072** ← BB91951419		2:57
11	CA collects all removed safe deposit box lock assemblies for future disposal.		2:57
~~12~~	~~CA takes each TEB containing a new safe deposit box lock assembly from the equipment cart and stores it in Safe 2.~~		
13	CA writes the date and time, then signs the safe log where "Replace Safe Deposit Box Lock Assemblies" is indicated. IW verifies the safe log entries, then initials it.		3:03

Verify New Combination and Close the Credentials Safe #2

Step	Activity	Initials	Time
14	SSC2 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.**		3:07
15	SSC2 performs additional tests on the dial if necessary. **Note: DO NOT Close the Safe door.**		3:10
16	SSC2 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.		3:10
17	SSC2 returns the safe log inside Safe #2, 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.		3:11

Test the Credentials Safe #2 and Exit the Safe Room

Step	Activity	Initials	Time
18	SSC2 opens Safe #2 while shielding the combination from the camera. **Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.**		3:13
19	SSC2 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.		3:13
20	SSC2 returns the safe log back to Safe #2, 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.		3:14
21	CA, IW, and any escorted personnel leave Tier 5 (Safe Room), returning to Tier 4 (Key Ceremony Room).		3:16

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.		3:17
2	CA calls each attendee on the participants list to proceed to the ceremony table and sign IW's participants list. **All signatures declare that this script is a true and accurate record of the ceremony.**		3:18
3	CA reviews IW's script, then signs the participants list.		3:19
4	IW signs the list and records the completion time.		3:20

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

Step	Activity	Initials	Time
5	CA requests that an SA stop the audit camera video recording.		3:20
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.)		3:20

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 (Appendix B). All TEBs are labeled **Root DNSSEC Administrative Ceremony Safe #2 Credentials Maintenance**, dated and signed by IW and CA. An off-site audit bundle is delivered to an off-site storage.		3:45

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 12