Root DNSSEC KSK

Administrative Ceremony
Safe #2 Credentials Maintenance

Tuesday 18 July 2023

Root Zone KSK Operator Key Management Facility
1920 East Maple Avenue, El Segundo, CA 90245, 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	Andres Pavez / PTI		2023 Jul 18	17:58
IW	Victoria Yang / ICANN			
SSC2	Anand Mishra / ICANN			
SA	Moises Cirilo / ICANN			
RKOS / IW Backup	Aaron Foley / PTI			
Locksmith	Richard Bowen / Industrial Lock and Security			
EW	Arbogast Fabian			
EW	Jorge Etges			
EW	Subramanian Moonesamy			

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 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.**	V Y	16:58
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.	V Y	16:58
3	CA asks that any first time ceremony participants in the room introduce themselves.	V Y	16:59

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
4	CA reviews emergency evacuation procedures with onsite participants.	V Y	16:59
5	CA explains the use of personal electronic devices during the ceremony.	V Y	16:59
6	CA summarizes the purpose of the ceremony.	V Y	17:00

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: 2023/7/18 17:00 **Note: All entries into this script or any logs should follow this common source of time.**	VY	17:00

Act 2: Safe #2 Credentials Maintenance

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

- Ensure the safe deposit box lock mechanisms are properly replaced

Open Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
1	CA and IW transport a flashlight, phillips screwdriver, safe deposit box TEB(s) and escort required personnel into Tier 5 (Safe Room.)	VY	17:02
2	SSC2 opens Safe #2 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.**	VY	17:04
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.	VY	17:05

Root DNSSEC Script Exception

Exception Details

Step	Activity	Initials	Time
1	IW writes the details of the ceremony exception: Act: 2 Step(s): 5 Page(s): 7 Date and Time: 17:28 **Note: IW describes the exception(s) and action(s) below.**	VY	17:54

During step 5, the lock in the bag BB46592072 didn't perform smoothly. We use bag BB91951423 for lock box #1793, and then continued with step 6. After replacing box #1789 with lock bag BB91951424, we locked the safe, exited the room and pick up a new lock. We reentered the room, replace box #1791 with lock bag BB91951425, and then resumed the ceremony.

Replace Safe Deposit Box Lock Assemblies

Step	Activity	Initials	Time
4	CA reads aloud TEB(s) #**BB91951424, BB91951423, and BB46592072** and along with IW checks for tamper evidence, then opens TEBs and places all contents on top of Safe 2 (Credentials Safe) for pending installation.	VY	17:06
5	The safe deposit box door and lock assembly are replaced by performing the following steps: a) Locksmith installs a new safe deposit box door and lock assembly. b) After the CA operates the guard key in the bottom lock, the CA closes the safe deposit box listed below, leaving the tenant keys installed in the lock. c) CA applies a **red** circular sticker to the door of the safe deposit box to denote the corresponding guard key. **Box # 1793** → BB91951423	VY	17:28
6	The safe deposit box lock assemblies are replaced 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 CA 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 # 1789** → BB91951424 → (VY: 17:33) **Box # 1791** → BB91951425 → (VY: 17:43)	VY	17:43
7	CA collects all removed safe deposit box lock assemblies for future disposal.	VY	17:44
8	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.	VY	17:44

Close Safe #2 (Tier 6, Credentials Safe)

Step	Activity	Initials	Time
9	SSC2 writes the date and time, then signs the safe log where **"Close Safe"** is indicated. IW verifies the safe log entry, then initials it.	VY	17:45
10	SSC2 returns the safe log 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.	VY	17:45
11	CA, IW, and any escorted personnel leave Tier 5 (Safe Room), returning to Tier 4 (Key Ceremony Room).	VY	17:46

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.	VY	17:55
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.**	VY	17:57
3	CA reviews IW's script, then signs the participants list.	VY	17:58
4	IW signs the list and records the completion time.	VY	17:58

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.	VY	17:59
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.)	VY	18:03

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 10). 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.	VY	18:15

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 10.

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

One set for the audit bundle.

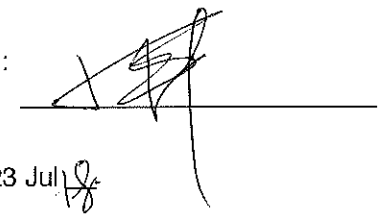
3. Other items

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: **Victoria Yang**

Signature: 

Date: 2023 Jul 18