Root DNSSEC KSK

Administrative Ceremony
RKSH6 Replacement

Thursday 25 April 2024

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

This ceremony is executed in accordance with the DNSSEC Practice Statement for the Root Zone KSK Operator 7th Edition (2024-03-15)

Abbreviations

AUD = Third Party Auditor
EW = External Witness
IW = Internal Witness
MC = Master of Ceremonies
RKSH = Recovery Key Share Holder
SA = System Administrator
SO = Security Officer
SW = Staff Witness
CA = Ceremony Administrator
FD = Flash Drive
KMF = Key Management Facility
OP = Operator
RKOS = RZ KSK Operations Security
SKR = Signed Key Response
SSC = Safe Security Controller
TCR = Trusted Community Representative
CO = Crypto Officer
HSM = Hardware Security Module
KSR = Key Signing Request
PTI = Public Technical Identifiers
RZM = Root Zone Maintainer
SMK = Storage Master Key
STM = Secure Transport Mode
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 time of completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Andres Pavez / PTI			
IW	Aaron Foley / PTI			
RKSH1 Successor	Sebastian Castro			
RKSH6 Current	Norm Ritchie			
RKSH6 Successor	John Curran			
EW	Rob Seastrom		2024 Apr 25	16:01
EW	Bevil Wooding			
EW	Kristian Ormen			
EW	Jiankang Yao			
SW	David Huberman			

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 begins recording with the audit cameras shortly before the ceremony begins
- 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 HSMs 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
- Explain the purpose of the ceremony along with a high-level list of tasks to be completed

Sign into Tier 4 (Key Ceremony Room)

Step	Activity	Initials	Time
1.1	CA confirms that required audit cameras are recording.		15:51
1.2	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.		15:53
1.3	CA asks that any first-time ceremony participants in the room introduce themselves.		15:53

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
1.4	CA reviews emergency evacuation procedures with onsite participants.		15:54
1.5	CA explains the use of personal electronic devices during the ceremony.		15:54
1.6	CA summarizes the purpose of the ceremony.		15:54

Verify the Time and Date

Step	Activity	Initials	Time
1.7	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: 2024 0425 15:55 **Note: All entries into this script or any logs should follow this common source of time.**		15:55

Trusted Community Representative Declaration

I understand that I will hold a trusted role in the Root Zone DNSSEC Key Signing Key operations, undertaken as a joint effort by the Root Zone Management Partners; Internet Corporation for Assigned Names and Numbers (ICANN), Public Technical Identifiers and Verisign.

Aside from background checks that were performed as part of the requirement from the DNSSEC Practice Statement (DPS) and the "trust" notion in becoming a Trusted Community Representative, I, **Sebastian Castro** uphold the highest honesty and integrity and hereby declare the following:

1. Within the past fifteen years, I have not been investigated for or convicted of a crime in any jurisdiction around the world related to fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

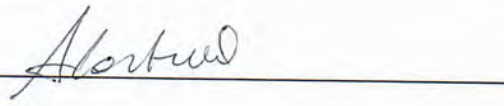
2. Within the past fifteen years, I have not been judged by any court or been the subject of any judicial determination, or in any type of dispute resolution proceeding, to have committed fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

3. Within the past fifteen years, I have not been disciplined by any government for conduct involving dishonesty, including, fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

4. I am currently not involved in any governmental, judicial, or regulatory proceeding or investigation that could result in a conviction, judgment, determination, or discipline of the type specified in 1, 2 or 3 above.

By signing this declaration, the undersigned attests that the aforementioned statements are true and accurate.

Date: 25-Apr-2024

Signature: 

Print name: **Sebastian Castro**

Trusted Community Representative Declaration

I understand that I will hold a trusted role in the Root Zone DNSSEC Key Signing Key operations, undertaken as a joint effort by the Root Zone Management Partners; Internet Corporation for Assigned Names and Numbers (ICANN), Public Technical Identifiers and Verisign.

Aside from background checks that were performed as part of the requirement from the DNSSEC Practice Statement (DPS) and the "trust" notion in becoming a Trusted Community Representative, I, **John Curran** uphold the highest honesty and integrity and hereby declare the following:

1. Within the past fifteen years, I have not been investigated for or convicted of a crime in any jurisdiction around the world related to fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

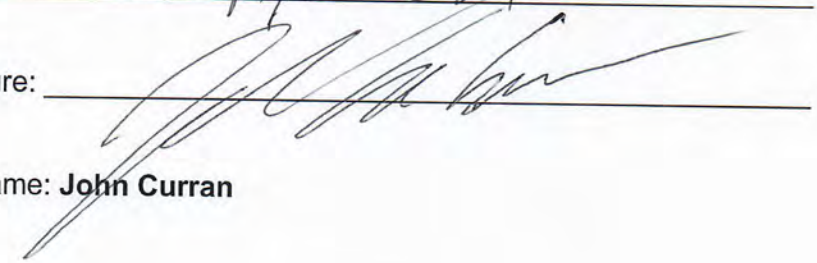
2. Within the past fifteen years, I have not been judged by any court or been the subject of any judicial determination, or in any type of dispute resolution proceeding, to have committed fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

3. Within the past fifteen years, I have not been disciplined by any government for conduct involving dishonesty, including, fraud, breach of fiduciary duty, theft of funds or other tangible or intangible property of others, conspiracy to commit a crime, or any other similar type of dishonest activity.

4. I am currently not involved in any governmental, judicial, or regulatory proceeding or investigation that could result in a conviction, judgment, determination, or discipline of the type specified in 1, 2 or 3 above.

By signing this declaration, the undersigned attests that the aforementioned statements are true and accurate.

Date: 25 April 2024

Signature: 

Print name: **John Curran**

Act 2: Recovery Key Share Holder Succession

Recovery Key Share Holder credentials will be transferred to a successor. A declaration form will be signed indicating the change, then the credentials are transferred to a successor.

Trusted Community Representative Declaration

Step	Activity	Initials	Time
2.1	CA confirms that the **Trusted Community Representative Declaration** forms are signed by the RKSH Successor. IW retains the original copy. **RKSH1 Successor: Sebastian Castro** **RKSH6 Successor: John Curran**		15:56

Transfer SMK to RKSH Successor

Step	Activity	Initials	Time
2.2	CA calls the RKSH Current and Successor to the ceremony table to perform the following steps: a) RKSH Current reads out the SMK TEB number, while IW verifies the information using the previous ceremony script where it was last used, then hands it to the CA. b) CA inspects SMK TEB for tamper evidence. c) CA gives the SMK TEB containing the SMK credentials to the RKSH Successor. d) RKSH Successor signs the IW's script where indicated. **RKSH6 Current: Norm Ritchie** **RKSH6 Successor: John Curran** **SMK TEB # A14377108** Signature:		15:58

Retiring TCR

Step	Activity	Initials	Time
2.3	CA acknowledges **Norm Ritchie** participation as one of the Trusted Community Representatives and presents them with a token of our appreciation.		15:59

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
3.1	CA reads all exceptions that occurred during the ceremony.		15:59
3.2	CA calls each in-person attendee not seated at the ceremony table to sign the IW's participant list. **All signatories declare to the best of their knowledge that this script is a true and accurate record of the ceremony.**		16:00
3.3	CA reviews IW's script, then signs the participants list.		16:00
3.4	IW signs the list and records the completion time.		16:01

Stop Recording

Step	Activity	Initials	Time
3.5	CA stops the audit camera video recording.		16:01

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 9.

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

One set for the audit bundle.

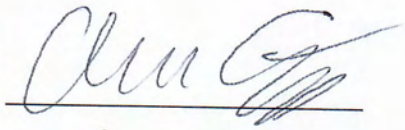
3. Audit Bundle Information

All TEBs are labeled **Root DNSSEC KSK Ceremony 53-1**, dated and initialed by IW and CA. An off-site audit bundle is delivered to an off-site storage.

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: 2024 Apr 25