Root DNSSEC
HSM Destruction

Wednesday February 7, 2018

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

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

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 found on https://www.iana.org/help/key-ceremony-roles
Instructions: At the end of the ceremony, participants sign on IW1's copy. IW1 records the time of completion.

Title / Roles	Printed Name	Signature	Date	Time
CA	Francisco Arias / ICANN		8 February 2018	02:12
IW1	Yuko Green / ICANN			
SSC1	Marilia Hirano / PTI			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian			
CO2	Dmitry Burkov			
CO3	Joao Damas			
CO4	Carlos Martinez			
CO5	Olafur Gudmundsson			
CO6	Nicolas Antoniello			
CO7	Subramanian Moonesamy			
RZM	Alejandro Bolivar / Verisign			
RZM	Duane Wessels / Verisign			
AUD	Victor kao / RSM			
AUD	Chris Koucheki / RSM			
SA1	Connor Barthold / ICANN			
SA2	Mike Brennan / ICANN			
CA2 / RKOS	Alberto Duero / PTI			
IW2 / RKOS	Andres Pavez / PTI			
SW	Jennifer Johnson / PTI			
SW	James Cole / ICANN			
SW	Audrey Fery-Forgues / ICANN			
EW	William Turton			
EW	Nathan Anderson			
EW	Matthew Justus			
Contractor	Oliver Kamenwa			
Contractor	~~Paul Kanja~~ Jose Ramos			
SW	Kim Davies			

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.

Note: The CA leads the ceremony. Dual Occupancy is enforced. Only CAs, IWs, or SAs can enter and escort other participants to the Ceremony room. Only CA + IW can enter the safe room and escort other participants. CAs, IWs, or SAs may escort participants out of the ceremony room at the CA's discretion and only when an IW + CA or SA remain inside the ceremony. No one may leave the Ceremony room if the safe room is occupied. All participants are required to sign in and out of the ceremony room using the visitor log. The SA starts filming before the participants enter the ceremony room.

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

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 the Administrative Ceremony

Sign into the Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are still recording and online video streaming is still active.	Y.G.	00:42
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the participants list on Page 2.	Y.G.	00:42

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	Y.G.	00:42
4.	CA briefly explains the purpose of the ceremony.	Y.G.	00:51

Verify the Time and Date

Step	Activity	Initials	Time
5.	IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2018/02/08 00:51 All entries into this script or any logs should follow this common source of time.	Y.G.	00:51

Act 2. Retrieve Zeroised HSMs

Open Equipment Safe #1

Step	Activity	Initials	Time
1.	CA, IW1 and SSC1 enter the safe room with a cart.	Y.G.	00:53
2.	SSC1 opens Safe #1 while shielding the combination from the camera.	Y.G.	00:53
3.	SSC1 takes out the existing safe log and shows the most recent page to the audit camera. IW1 provides a blank pre-printed safe log to the SSC1. SSC1 writes the date/time and signature on the safe log where "Open Safe" is indicated. IW1 verifies this entry then initials it.	Y.G.	00:54

Remove the HSMs from Safe #1

Step	Activity	Initials	Time
4.	CA extracts the zeroised HSMs from the safe by following the steps below: a) Remove the HSM in TEBs listed below from the safe. b) Read out the TEB serial number, then verify its integrity while showing it to the audit camera. c) Place the HSM TEB on the cart. d) Write the date/time and signature on the safe log where "**Remove HSM**" is indicated. e) IW1 verifies the safe log entry, then initials it. HSM1: **TEB# BB24646623 / serial # K6002020** ✓ HSM2: **TEB# BB24646624 / serial # K6002018**	Y.G.	00:56

Close the Equipment Safe #1

Step	Activity	Initials	Time
5.	SSC1 writes the date/time and signature on the safe log where Close Safe is indicated. IW1 verifies this entry, then initials it.	Y.G.	00:57
6.	SSC1 returns the safe log back in the Safe #1 and locks it (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verifies that the safe is locked and the "WAIT" light indicator is off.	Y.G.	00:57
7.	CA, SSC1 and IW1 leaves the safe room with the cart, closing the door behind them.	Y.G.	00:58

Act 3. Destroy the Zeroised HSMs

Prepare HSMs for Destruction

Step	Activity	Initials	Time
1.	CA prepares the HSMs by following the steps below: a) Read out the TEB # and the serial # while IW1 matches it with the Root DNSSEC KSK Ceremony 26 script. b) Remove and discard the TEBs, then place both HSMs on the table. HSM1: **TEB# BB24646623 / serial # K6002020** HSM2: **TEB# BB24646624 / serial # K6002018**	Y.G.	01:00
2.	CA verifies the tamper indicator "**ALERT**" LED by following the steps below: a) Connect the power to the HSM, then wait for it to display "Important Read Manual" which indicates not tampered b) Push the pinhole button behind the HSM, then release it after 10 seconds to tamper it. c) Press "RESTART" and wait until the "**ALERT**" LED light is **ON**. d) Disconnect the power from the HSM **Note:** The HSM is tampered when the Alert LED is ON.	Y.G.	01:04

Step	Activity	Initials	Time
3.	**Note:** IW1 reads the remaining steps 3 to 7 while CA prepares the HSMs for destruction. CA removes the HSM's top enclosure by following the steps below: a) Remove (8) screws that hold the enclosure using Tool A. b) Remove (2) screws that hold the serial port using Tool B. c) Remove (2) screws on the power port of the HSM using Tool C. d) Break the tamper sticker at the bottom, then slide the enclosure. e) Remove (2) screws that hold the interface board using Tool C, then remove the plastic cover. f) Remove the remaining (2) screws that hold the interface board. g) Detach (4) cables from the interface board.	Y.G.	01:10
4.	CA removes the interface board and battery by following the steps below: a) Cut the (2) zip ties using Tool D b) Pry the rear enclosure of the HSM using Tool E c) Separate the interface board from the HSM enclosure d) Cut both gold and green cables between the crypto module and the interface board using Tool D. e) Cut the battery terminals from the interface board using Tool D, then detach the battery. f) Provide RKOS the battery for proper disposal.	Y.G.	01:16
5.	CA removes the cryptographic module by following the steps below: a) Remove (4) nuts that hold the module using Tool F or Tool E b) Detach the module from the enclosure	Y.G.	01:19
6.	CA removes the front panel and card reader by following the steps below: a) Remove (4) nuts that hold the front panel from the enclosure base using Tool F, then separate it. b) Remove (3) screws and (1) nut that secure the card reader using Tool C and Tool F respectively.	Y.G	01:24
7.	~~Repeat steps 3 to 6 for the 2nd HSM.~~		

Destroy HSMs

Step	Activity	Initials	Time
8.	CA collects the following parts from both HSMs to prepare for destruction. a) Cryptographic Module b) Interface Board c) Card Reader d) Front Panel and internal cables	Y.G.	01:25
9.	CA and Contractor performs the destruction of each HSM part repeatedly.	Y.G.	01:55
10.	CA and IW1 collects all destroyed HSM parts using bag(s), then gives it to RKOS for proper disposal.	Y.G	01:58
11.	Contractor provides the hardware destruction certificate for IW1 to attach to the script.	Y.G.	01:59

Act 4. Close the Ceremony

Participant Signing of IW1's Script

Step	Activity	Initials	Time
1.	CA calls each attendee on the participants list to proceed to the ceremony table and **sign IW1's participants list. All signatures declare that this script is a true and accurate record of the ceremony.** IW1 records the completion time once all participants have signed the list.	Y.G	02:12
2.	CA reviews IW1's script and signs the participants list.	Y.G.	02:13

Stop Online Streaming

Step	Activity	Initials	Time
3.	CA acknowledges all participants both online and on-site, then notifies the SA to stop the online streaming.	Y.G.	02:13

Post Ceremony Information

Step	Activity	Initials	Time
4.	CA informs onsite participants about post ceremony activities.	Y.G.	02:15

Sign Out of Ceremony Room and Stop Video Recording

Step	Activity	Initials	Time
5.	RKOS ensures that all participants sign out of the Ceremony Room log and are then escorted out of the Ceremony Room. SA, IW1 and CA remain in the Ceremony Room.	Y.G	02:50
6.	CA notifies the SA to stop video recording.	Y.G	02:51

Root DNSSEC Script Exception

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

E1

Instructions: Initial each step that has been completed below. Note time.

Note Exception Time

Step	Activity	Initials	Time
1.	IW1 notes date and time of key ceremony exception and signs here: 2018/02/08 00:47	Y.G.	00:49
2.	IW1 Describes exception and action below.	Y.G.	00:51

Instead of destroying two HSMs. We will only destroy one today. ~~The other one~~ We will determine what to do with the undestroyed one at a later time. ~~This is with the intention of COA~~

– End of Root DNSSEC Script Exception –

Root DNSSEC Script Exception

Abbreviations

TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

E2

Instructions: Initial each step that has been completed below. Note time.

Note Exception Time

Step	Activity	Initials	Time
1.	IW1 notes date and time of key ceremony exception and signs here: 2016/02/08 01:54	Y.G.	01:54
2.	IW1 Describes exception and action below.	Y.G.	01:57

BB51184701

Exception to step 10. Instead of giving the destroyed HSM1 to RKOS for disposal, we ~~will~~ have collected the destroyed pieces in the tamper evidence bag and stored it in the safe. The TEB# is shown above.

– End of Root DNSSEC Script Exception –

SHRED TIME

CERTIFICATE OF DESTRUCTION

This is to certify that all confidential hardware entrusted to ***Shred-Time***

By: **Public Technical Identifiers (PTI)**

Address: 12025 Waterfront Dr., Suite 300, Los Angeles, CA 90094

Invoice #: *4918* **Service:** *Destruction of Hardware*

Have been handled with the highest degree of security and completely destroyed by a physical destruction process.

Supervised & Certified By: Oliver Kamenwa **Date Destroyed: Feb 7th, 2018**

Type of Material Destroyed: *Hardware Security Module (HSM)*

***Module**: Keyper Professional 9720*

***Serial No.**: K6002020*

5451 W. 104TH Street, Los Angeles, CA 90045. Tel: (310)348-9773 Fax: (310)348-9723

.....confidentiality is our priority!! www.Shred-time.com

CORPORATE SEAL