



Internet Corporation for Assigned Names and Numbers

**Root DNSSEC
Crypto Officer Recovery
Thursday February 11, 2016**

**ICANN KSK Facility@Equinix LA3
1920 East Maple Avenue, El Segundo, CA 90245**

**This operation and maintenance is executed under the
DNSSEC Practices Statement for the Root Zone KSK Operator Version A Revision 1358**



Abbreviations

- TEB = Tamper Evident Bag (AMPAC, item #GCS1013, item #GCS0912 small or #GCS1216 large or MMF Industries, item #2362010N20 small or #2362011N20 large)
- OP = Operator
- SW = Staff Witness
- MC = Master of Ceremony
- AUD = Third Party Auditor
- FD = Flash Drive
- SO = Security Officer
- CA = Ceremony Administrator
- SSC = Safe Security Controller
- IKOS = ICANN KSK Operations Security
- RZM = Root Zone Maintainer
- KSR = Key Signing Request
- CO = Crypto Officer
- IW = Internal Witness
- EW = External Witness
- SA = System Administrator
- HSM = Hardware Security Module
- SKR = Signed Key Response

Participants

Instructions: At the end of the ceremony, participants sign on IW1's copy. IW1 records time upon completion.

Title	Printed Name	Signature	Date	Time
CA	Kim Davies / ICANN		11 February 2016	
IW1	Yuko Green / ICANN			
SSC1	Marilyn Hirano / ICANN			
SSC2	Flauribert Takwa / ICANN			
CO1	Arbogast Fabian / TZ			
CO2	Dmitry Burkov / RU			
CO3	Joao Damas / PT			
CO6 Successor	Nicolas Antonello / UY			
CO7	Subramanian Moonesamy / MU			
RZM	Alejandro Bolivar / Verisign			
RZM	Duane Wessels / Verisign			
RZM	Sanju Varghese/ Verisign			
RZM	Brad Verd / Verisign			
AUD	Jackie Kwong / PricewaterhouseCoopers			
AUD	Abbey Beam / PricewaterhouseCoopers			
SA1	Connor Barthel / ICANN Erian Martin			
SA2	Josh Jenkins / ICANN			
CA2 / IKOS	Alberto Duero / ICANN			
IW2 / IKOS	Andres Pavez / ICANN			
CA3	Edward Lewis / ICANN			
EW	Reg Levy			
EW	James Gannon			
Locksmith	Rich Bowen / Industrial Lock and Security			
SW	Sabrina Tanamal			

Note: By signing this script, you are declaring that this is a true and accurate record of the Root DNSSEC KSK ceremony to the best of your knowledge.



Note: Dual Occupancy enforced. CA leads ceremony. Only CAs, IWs, or SAs can enter ceremony room and/or escort other participants. Only CA+IW can enter safe room and/or escort other participants. CAs, SAs or IWs may let individuals out of the ceremony room but only when CA+IW remain in the ceremony room. No one may leave when CA+IW are in safe room. Participants must sign in and out of ceremony room and leave any credentials assigned to them (keys, cards) in the ceremony room if leaving before completion of the ceremony. The SA starts filming before the participants enter the room.

Some steps during the ceremony require the participants to tell and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the phonetic alphabet shown below will 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 Crypto Officer Recovery

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.	Y.G	21:01
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.	Y.G	21:05

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	Y.G	21:06
4.	CA explains the use of personal electronics devices during the ceremony.	Y.G	21:07
5.	CA briefly explains the purpose of the ceremony.	Y.G	21:09

Verify Time and Date

Step	Activity	Initials	Time
6.	<p>IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room:</p> <p>Date and time: <u>11 February 2016 21:10</u></p> <p>All entries into this script or any logs should follow this common source of time.</p>	Y.G	21:10

Confirm the Trusted Community Representatives Declaration

Step	Activity	Initials	Time
7.	CA confirms the <i>Trusted Community Representative Agreement</i> is signed and submitted by the CO6 Successor.	Y.G	21:12



Act 2. Drill the Safe Deposit Box Lock, verify the OP and SO Credentials inside the TEB

Open Credential Safe #2

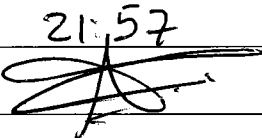
Step	Activity	Initials	Time
1.	CA and IW1 escort SSC2, CO6 Successor , and locksmith into the safe room together. CA brings a flashlight and the pre-labeled "SPARE TEB" when entering the safe room. Note: Spare TEB will ONLY be used if the drilled lock's metal shavings damage the existing TEB.	Y.G.	21:14
2.	SSC2, while shielding combination from camera, opens Safe #2.	Y.G.	21:15
3.	SSC2 takes out the existing safe log and prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	Y.G.	21:16

Locksmith Drills the Safe Deposit Box Locks and CO6 Successor verifies the OP and SO TEB

Step	Activity	Initials	Time
4.	CA confirms the safe deposit box number that needs to be drilled. Then Locksmith carefully drills and opens the safe deposit box. Box 1072 (due to Crypto Officer Recovery)	Y.G.	21:46
5.	The CO6 Successor checks the OP and SO TEB and retrieves both TEB following the steps shown below a) Verify integrity of contents by reading out box number and TEB # for OP and SO which should match below. b) Makes an entry in safe log indicating OP and SO TEB removal with box #, printed name, date, time and signature. Note: If log entry is pre-printed, verify the entry, record time of completion and sign. IW1 initials this entry. CO6 Successor: Nicolas Antonello Box # 1072 (Old box) OP TEB # BB21368989 SO TEB # BB21907266	Y.G.	21:48
6.	Locksmith removes the drilled dual nose Mosler locks from the safe deposit box and installs a new unit leaving the new key into the lock. Box 1072 (due to Crypto Officer Recovery)	Y.G.	21:53



CO6 Successor Receive New Safe Deposit Box Keys and Return OP and SO TEB

Step	Activity	Initials	Time
7.	<p>CO6 Successor:</p> <p>a) Opens the safe deposit box, using one of the keys already in place, with assistance of CA who uses his/her common key, and looks into the box with a flashlight to verify that the box is empty.</p> <p>b) Closes and locks the box and opens and closes it once again to test his/her second key, with the assistance of the CA and his/her common key.</p> <p>c) CO6 Successor makes an entry into the safe log indicating the return of OP and SO TEB including Box #, TEB #, card type, printed name, date, time, and signature. IW1 initials the entry after verifying contents and integrity of the TEB and comparing TEB# s and card type to his/her script. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>d) CO6 Successor shows the bag to the camera and then places his/her TEB into his/her box and locks the safe deposit box with the help of the CA.</p> <p>e) Enters the box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # 1073 (New box) Printed Name Nicolas Antonello Date February 11, 2016</p> <p>Time _____ 21:57 _____ Signature _____  _____</p>	Y.G.	21:57



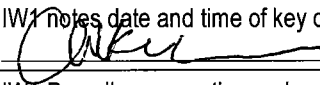
ICANN DNSSEC Script Exception

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

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

Note Exception Time

Step	Activity	Initials	Time
1.	IWI notes date and time of key ceremony exception and signs here: 	Y. G.	22:08
2.	IWI Describes exception and action below.		

Step 13:

Lock smith will stay until the next ceremony's key using / lock opening to ensure that there is no issue with locks or keys. This is due to all the banging that took place to replace the key.

– End of DNSSEC Script Exception –



Close Credential Safe #2

Step	Activity	Initials	Time
8.	Once all safe deposit boxes are closed and locked, SSC2 makes an entry that includes printed name, date, time and signature into the safe log indicating closing of the safe. IW1 initials this entry. Note: If log entry is pre-printed, verify the entry, record time of completion and sign.	Y.G	21:58
9.	SSC2 puts log back in safe and locks Safe #2 (spin dial at least two full revolutions each way, counter clock wise then clock wise). CA and IW1 verify that the safe is locked and card reader indicator is green.	Y.G.	21:59
10.	CA, IW1, SSC2, CO6 Successor and locksmith leaves the safe room, closing the door behind them.	Y.G.	21:59

Participant Signing of IW1's Script

Step	Activity	Initials	Time
11.	One by one, all participants come to the front of the room, confirms printed name and date. Then, the participant declares that this script is a true and accurate record of the ceremony by signing on IW1's script coversheet. IW records the completion time once all participants have signed the coversheet. Note: If entry is pre-printed, verify the entry and sign.	Y.G	22:05
12.	CA reviews IW1's script and signs it.	Y.G.	22:06

Locksmith Signing Out of Ceremony Room

Step	Activity	Initials	Time
13.	IKOS ensures that the locksmith sign out of Ceremony Room log and is escorted out of the Ceremony Room. All participants remain in the Ceremony Room.		

Continue to Root DNSSEC KSK Ceremony 24 when IKOS Returns to the Ceremony Room



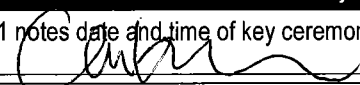
ICANN DNSSEC Script Exception

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

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: 	Y.G.	22:13
2.	IW1 Describes exception and action below.		

22:10 Exit door was forced open by a participant leaving Tiger 4 by accident.

– End of DNSSEC Script Exception –