



Internet Corporation for Assigned Names and Numbers

**Root DNSSEC
Crypto Officer Rotation and
Safe Deposit Box Maintenance**

Thursday May 2, 2013

ICANN KSK Facility@Terremark NCR
18155 Technology Drive, Culpeper, VA 22701-3805

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



AbbreviationsDraft

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

Participants

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

Title	Printed Name/Citizenship	Signature	Date	Time
CA	Mehmet Akcin		2 May 2013	17:52
IW1	Francisco Arias			
SA1	Alexander Kulik			
SSC1	Julie Hedlund			
SSC2	Patrick Jones			
SA2	Matt Childs			
CO3	Olaf Kolkman / NL			
CO4	Robert Seastrom / US			
CO5	Christopher Griffiths / US			
CO6	Gaurab Upadhaya / NP			
Secure Key Courier	Russ Housley / Vigil Security			
EW1	Alejandro Bolivar / Verisign			
EW2	Sanju Varghese / Verisign			
EW3	Randy Whitney / Verizon Business			
EW4	James Anderson / Neustar			
EW5	Edward Lewis / Neustar			
EW6	Mostafa Elghazaly / PricewaterhouseCoopers			
EW7	Sonia Wong / PricewaterhouseCoopers			
EW8	Olafur Gudmundsson/Shinkuro			
IW2/IKOS	Tomofumi Okubo			
Locksmith	Billy Schopsel / Professional Lock	FA		

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 CO Rotation and Maintenance

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initial	Time
1.	SA starts video recording and online streaming. SAs or IWs escort participants into the Ceremony Room and all participant sign into the Ceremony Room log.	FA	17:07

Emergency Evacuation Procedures

Step	Activity	Initial	Time
2.	CA or IW reviews emergency evacuation procedures with participants.	FA	17:10

Verify Time and Date

Step	Activity	Initial	Time
3.	IW1 enters UTC date (day/month/year) and time using a reasonably accurate wall clock visible to all in the Ceremony Room: Date and time: <u>2 May 2013 17:12</u> All entries into this script or any logs should follow this common source of time.	FA	17:12

Confirm the TCR CO Rotation Exemption Attestation

Step	Activity	Initial	Time
4.	IW and CA confirm the <i>Trusted Community Representative Crypto Officer Rotation Exemption Attestation</i> is signed by the departing CO5.	FA	17:13
5.	Secure Key Courier confirms and signs the attestation and hands safe deposit box keys to the entering CO5.	FA	17:14



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, e.g., *BTS*. Note time.

Note Exception Time

Note Exception Time			
1	IW notes date and time of key ceremony exception and signs here:	FA	17:19
2	IW Describes exception and action below		

- Before entering tier 5 (step 6) we realize the lack of pre-printed logs. The IKOS printed a set for IW.

– End of DNSSEC Script Exception –

Act 2. Verify the OP and SO Credentials

Open Credential Safe #2

Step	Activity	Initial	Time
6.	CA and IW1 escort SSC2, all COs, Secure Key Courier and locksmith into the safe room together. CA brings a flashlight when entering the safe room.	FA	17:27
7.	SSC2, while shielding combination from camera, opens Safe #2.	FA	17:29
8.	SSC2 takes out safe log and prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry. <i>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</i>	FA	17:29

CO5 verifies the OP and SO credentials

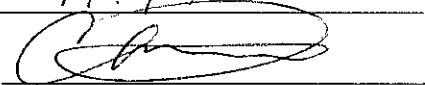
Step	Activity	Initial	Time
9.	CO5 checks the OP/SO cards and retrieves both cards following the steps shown below a) With the assistance of CA (and his/her common key), opens her/his safe deposit box. # Common Key is bottom lock and CO Key is top lock b) Verifies integrity of contents by reading out box number and TEB # for OP and SO cards which should match below. c) Makes an entry in safe log indicating OP and SO TEB removal with box #, printed name, date, time and signature. <i>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</i> IW1 initials this entry. CO 5: Christopher Griffiths Box # 1240 OP TEB # A15473416 SO TEB # A14377125	FA	17:33
10.	CO5, together with the Secure Key Courier and other COs onsite verifies the integrity of the TEBs. Once CO5 is comfortable with the integrity of the credentials, signs off the attestation to complete the CO rotation.	FA	17:34

Locksmith Replaces the Safe Deposit Box Locks

Step	Activity	Initial	Time
11.	CA confirms that the boxes below are empty then the Locksmith removes the dual nose Mosler locks from the safe deposit box and installs new units. The box that needs replacement is as below. Box 1240 (due to Crypto Officer Rotation) Box 1241 (due to malfunctioning Lock)	FA	17:41



CO5 Receive New Safe Deposit Box Keys and Return OP and SO Cards

Step	Activity	Initial	Time
12.	<p>CO5:</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) CO5 makes an entry into the safe log indicating the return of OP and SO card 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.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p> <p>d) CO5 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 # 1240</p> <p>Printed Name Christopher Griffiths</p> <p>Date 2 May, 2013</p> <p>Time 17:44</p> <p>Signature </p>	FA	17:44

Close Credential Safe #2

Step	Activity	Initial	Time
13.	<p>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.</p> <p>Note: If log entry is pre-printed, verify the entry, record time of completion and sign.</p>	FA	17:44
14.	<p>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).</p> <p>CA and IW1 verify that the safe is locked and card reader indicator is green.</p>	FA	17:45
15.	<p>IW1, CA, SSC2, and all COs, Secure Key Courier and locksmith leave safe room, closing the door behind them.</p>	FA	17:46
16.	<p>SA escorts the locksmith out of the key management facility</p>	FA	17:47



Participant Signing of IW1's Script

Step	Activity	Initial	Time
17.	ICANN KSK Operations Security confirms that CO rotation is perform in accordance with the exemption attestation and signs off.	FA	17:48
18.	All participants enter printed name, date, time, and signature on IW1's script coversheet. The <i>Trusted Community Representative Crypto Officer Rotation Exemption Attestation</i> is to be filed in the audit bundle with this script.	FA	17:53
19.	CA reviews IW1's script and signs it.	FA	17:55

Continue to Root DNSSEC KSK Ceremony 13



ICANN Trusted Community Representative
Crypto Officer Rotation Exemption Attestation


To Whom It May Concern,

This document identifies and attests to the procedure for the Trusted Community Representative (TCR) Crypto Officer Rotation of Crypto Officer (CO) 5 of 7 performed on May 2, 2013 in Culpeper VA, U.S.A.

The Secure Key Courier, Russ Housley will transfer the safe deposit key to the ICANN KSK Facility that resides on 18155 Technology Drive, Culpeper, VA Terremark NCR on behalf of the departing Crypto Officer 5 of 7, Vinton Cerf. The Departing Crypto Officer 5 of 7, Vinton Cerf will step down from the TCR role upon successful delivery of the safe deposit key to the Entering Crypto Officer 5 of 7, Christopher Griffiths. The Entering Crypto Officer 5 of 7, Christopher Griffiths will accept the TCR role upon receiving the safe deposit key from the Secure Key Courier, Russ Housley.

As Trusted Community Representative Departing Crypto Officer 5 of 7, I, Vinton Cerf have authorized and delegated the transfer of the safe deposit box key to the Secure Key Courier, Russ Housley. Upon the delivery of the safe deposit box key to the Entering Crypto Officer 5 of 7, Christopher Griffiths, I have agreed to step down from the role of Trusted Community Representative Crypto Officer 5 of 7.

Name Vinton Cerf

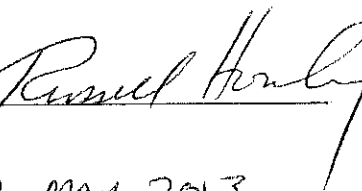
Signature 

Role Departing Crypto Officer 5 of 7

Date 4/27/2013

I, Russ Housley as the Secure Key Courier, confirm that the safe deposit box key was always under my control after receiving it from the Departing Crypto Officer 5 of 7, Vinton Cerf and was kept safe in a reasonable manner while in my custody.

Name Russ Housley

Signature 

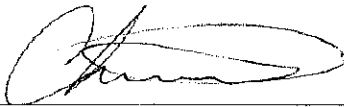
Role Secure Key Courier

Date 2 MAY 2013



I, **Christopher Griffiths** as the **Entering Crypto Officer 5 of 7**, have agreed to accept all responsibilities associated with the role of Trusted Community Representative Crypto Officer 5 of 7 once I have received the safe deposit box key from **Secure Key Courier, Russ Housley** and confirmed the contents of the safe deposit box with the **Secure Key Courier, Russ Housley** and the other Crypto Officers that are onsite for this transfer.

Name **Christopher Griffiths**

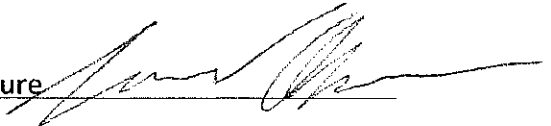
Signature 

Role **Entering Crypto Officer 5 of 7**

Date **5/2/2013**

I attest that the foregoing information is true and valid to the best of my knowledge,

Name **Tomofumi Okubo**

Signature 

Role **ICANN KSK Operations Security**

Date **5/2/2013**