



## Instructions for DNSSEC Key Ceremony Participants

As a participant in a DNSSEC Key Ceremony you do not need to prepare or bring anything but yourself and any credential (smartcard or physical key) that was assigned to you in a prior ceremony. "Key Ceremony" is a term of art used to describe a meeting of the individuals required to generate or use digital keys that the public will rely on – in this case, the DNSSEC Root key. The goal of such a ceremony is to get people to trust the key, and therefore use it, by making the process as transparent as possible. The event will be audited by a third party and filmed for the wider Internet community to see.

### What you need

You will need Government issued I.D. to enter the secure building and any credentials (physical key or smartcard) that you may have been assigned in a prior key ceremony.

### Locations

Terremark Datacenter  
18155 Technology Dr, Culpeper, VA, 22701, USA

LAX Datacenter  
1920 E Maple Ave, El Segundo, CA, 90245-3411, USA  
(Nearest cross street: Sepulveda/Maple)

Your participation is both critical and deeply appreciated. If you have any questions please feel free to contact the ICANN Key Manager.

### Ground rules

This very first Key Ceremony will last approximately 6 hours. There will be one break in the middle of the Key Ceremony allowing you to leave the room. You must leave all credentials before you each sign out of the Ceremony Room logbook. You may use the same line to sign out as you initially signed into the room. Leave all credentials that have been handed to you on the table at the front of the room. The materials will be watched by the Ceremony Administrator (CA) and Internal Witness (IW) in your absence. On return please make sure to pick up the same credentials (bags, keys, etc) that were originally handed to you. You must be escorted out of the room. You must also be escorted on return and sign back in to the ceremony room log book.

There may also be breaks between elements during the ceremony when you can stretch your legs and ask questions. Unless there is something you see in error please hold questions until these breaks.

Dual Occupancy requirements are in force. Violation of these requirements will trigger audible and visible alarms. PLEASE FOLLOW THE INSTRUCTIONS OF ICANN STAFF. Should an alarm trigger, we may be forced to scrap the Key Ceremony and start over. CA or Master of Ceremonies (MC) lead ceremony. Only CA + IW or System Administrator (SA) + IW can enter ceremony room (Tier 4). Only CA+IW can enter safe room (Tier 5). SA or IW may let individuals in



and out of the ceremony room but only when CA+IW are 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. If any of these conditions are not met, a warning siren is emitted until the situation is corrected.

### **What to focus on**

As a representative of the community it is your job to make sure things are done right by supplying your credentials and witnessing the procedures. So please watch each procedure carefully as the MC+CA explain what is being done. Transparency is a key element of the ceremony. If some part of it does not make sense, ask questions at the break.

Attached you will find the steps that will be performed in today's key ceremony. Use it to follow along making notes as needed. Although you are free to take this and any other material handed out during the ceremony, the notes you make on improving the ceremony will be greatly appreciated.

### **Roles you may have**

#### ***External Witness (EW)***

The External Witnesses observes the key ceremony and attests that it has been executed as described in the key ceremony procedure.

External Witnesses represent 3rd parties and are not affiliated with ICANN. An auditor would, in this context, be considered an External Witness.

#### ***Crypto Officers (CO)***

Crypto Officers hold a key to a safe deposit box placed inside Safe 2. The safe deposit boxes contains the credentials (in tamper evident packaging) needed for the Crypto Officer to authenticate with the Hardware Security Module.

Crypto Officers are Trusted Community Representatives, representing the technical DNS community.

The Crypto Officer is a trusted role.

Seven (7) Crypto Officers are required per site. However, only any three (3) are required to perform operations. Crypto Officers may not serve multiple sites.

#### ***Recovery Key Share Holders (RKSH)***

Each Recovery Key Share Holder holds a key to a bank safe deposit box under their control containing a smartcard (in tamper-evident packaging) holding part of the HSM internal encryption key.

The Recovery Key Share holder is required to provide and maintain records of where the smartcard is stored, and to participate in an annual inventory.

The Recovery Key Share Holder is a trusted role.

Seven (7) Recovery Key Share Holders in total are required, and are common for all sites. Only any five (5) are required to perform restoration operations.

**– End of Instructions –**



## ICANN DNSSEC Key Ceremony Scripts

### 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

### Participants

**Instructions:** At the end of the ceremony, participants print name, citizenship, signature, date, time, and time zone on IW1's copy.

Title	Printed Name/Citizenship	Signature	Date	Time
Sample	Bert Smith	<i>Bert Smith</i>	16 Jun 2010	18:00 UTC
MC	Richard Lamb /US	<i>Richard Lamb</i>	17 Jun 2010	00:02 UTC
CA	Mehmet Akcin /US	<i>Mehmet Akcin</i>	17 Jun 2010	00:02 UTC
IW1	Francisco Arias /MX	<i>Francisco Arias</i>	17 Jun 2010	00:02
IW2	Kim Davies /AU	<i>Kim Davies</i>	17 June 2010	0:03
IW3	Craig Schwartz / US	<i>Craig Schwartz</i>	17 June 2010	0:03
SA1	Reed Quinn /US	<i>Reed Quinn</i>	17 June 2010	00:012
SA2	Tom Berens /US	<i>Tom Berens</i>	17 Jun 2010	0:12
SSC1	Alexander Kulik /US	<i>Alexander Kulik</i>	17 June 2010	0:11
SSC2	Patrick Jones /US	<i>Patrick Jones</i>	17 Jun 2010	00:04
CO1	Frederico Neves /BR	<i>Frederico Neves</i>	17 Jun 2010	00:08
CO2	Ann-Marie Eklund Lowinder /SE	<i>Ann-Marie Eklund Lowinder</i>	17 June 2010	00:09
CO3	Olaf Kolkman /NL	<i>Olaf Kolkman</i>	17 Jun 2010	00:09
CO4	Robert Seastrom /US	<i>Robert Seastrom</i>	17 Jun 2010	00:10
CO5	Vinton Cerf /US	<i>Vinton Cerf</i>	17 June 2010	0:05
CO6	Gaurab Upadhaya /NP	<i>Gaurab Upadhaya</i>	17 Jun 2010	00:06
CO7	Christopher Griffiths /US	<i>Christopher Griffiths</i>	17 June 2010	00:06
RKSH1	Moussa Guebre /BF	<i>Moussa Guebre</i>	17 June 2010	00:06
RKSH2	Ondrej Sury /CZ	<i>Ondrej Sury</i>	17.6.2010	00:07
RKSH3	Paul Kane /UK	<i>Paul Kane</i>	17 June 2010	0:07
RKSH4	Jiankang Yao /CN	<i>Jiankang Yao</i>	17 Jun 2010	0:03
RKSH5	Bevil Wooding /TT	<i>Bevil Wooding</i>	17 Jun 2010	0:07



Title	Printed Name/Citizenship	Signature	Date	Time
RKSH6	Norm Ritchie /CA	<i>[Signature]</i>	17-Jun	00:04
RKSH7	Dan Kaminsky /US	<i>[Signature]</i>	16-Jun	23:35
EW1	Matt Larson /US	<i>[Signature]</i>	17-Jun	01:05
EW2	Ken Michaels /US	<i>[Signature]</i>	17-JUN	01:05
EW3	Jakob Schlyter /SE	<i>[Signature]</i>	17 Jun 10	01:09
EW4	Fredrik Ljunggren /SE	<i>[Signature]</i>	17 Jun 10	01:10
EW5	David Lawrence /US	David Lawrence	17 Jun	01:06
EW6	AINA ACATN	<i>[Signature]</i>	17 June	01:06

Note: Dual Occupancy enforced. CA leads ceremony. Only CAs, IW s, or SAs can enter ceremony room and/or escort other participants. Only CA+IW can enter safe room. 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.

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

### Prologue Script

#### Participants Arrive

Step	Activity	Initial	Time
1	SAs or IWs escort participants into the Ceremony Room.	FA	17:25

#### Sign into Key Ceremony Room

Step	Activity	Initial	Time
2	SA and IW2 have all participants sign into the Ceremony Room log.	FA	17:25

#### Emergency Evacuation Procedures

Step	Activity	Initial	Time
3	CA or MC review emergency evacuation procedures with participants.	FA	17:26

#### Verify Time and Date

Step	Activity	Initial	Time
4	IW1 enters date (month/day/year), UTC time using a reasonably accurate wall clock visible to all here: Date (UTC): <u>16 June 2010</u> Time (UTC): <u>17:27</u> All entries into this script or any logs should follow this common source of time.	FA	17:27



Open Credential Safe #2

Step	Activity	Initial	Time
5	CA and IW1 escort SSC2 and all COs into the safe room together.	FA	17:28
6	SSC2, while shielding combination from camera, opens Safe #2.	FA	17:29
7	SSC2 takes out safe log and prints name, date, time, signature, and reason (i.e. "open safe") in safe log. IW1 initials this entry.	FA	17:31

Hand Out Safe Deposit Box Keys (Approximately 3 minutes per CO = 21 minutes)

Hand out key to CO1

Step	Activity	Initial	Time
8	<p>CO1:</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) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry.</p> <p>d) Enters the same data with box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # <u>1238</u></p> <p>Printed Name <u>Frederico Neves</u></p> <p>Date <u>16062010</u></p> <p>Time <u>1733</u></p> <p>Signature <u>Frederico Neves</u></p>	FA	17:33

Hand out key to CO2

Step	Activity	Initial	Time
9	<p>CO2:</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) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry.</p> <p>d) Enters the same data with box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # <u>1259</u></p> <p>Printed Name <u>Ann-Marie Eklund Lowinder</u></p> <p>Date <u>16 June 2010</u></p>	FA	17:56



Step	Activity	Initial	Time
	Time <u>17:36</u> Signature <u>[Handwritten Signature]</u>		

**Hand out key to CO3**

Step	Activity	Initial	Time
10	<p>CO3:</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) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry.</p> <p>d) Enters the same data with box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # <u>1239</u></p> <p>Printed Name <u>Olaf Kolkman</u></p> <p>Date <u>16 JUNE 2010</u></p> <p>Time <u>17:38</u></p> <p>Signature <u>[Handwritten Signature]</u></p>	FA	17:39

**Hand out key to CO4**

Step	Activity	Initial	Time
11	<p>CO4:</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) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry.</p> <p>d) Enters the same data with box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # <u>1260</u></p> <p>Printed Name <u>Robert Seastrom</u></p> <p>Date <u>16 JUNE 2010</u></p> <p>Time <u>1740 UTC</u></p> <p>Signature <u>[Handwritten Signature]</u></p>	FA	17:41



**Hand out key to CO5**

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) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry.</p> <p>d) Enters the same data with box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # <u>2240</u></p> <p>Printed Name <u>Vinton Cerf</u></p> <p>Date <u>6-16-2010</u></p> <p>Time <u>17:41</u></p> <p>Signature <u>[Signature]</u></p>	FA	17:42

**Hand out key to CO6**

Step	Activity	Initial	Time
13	<p>CO6:</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) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry.</p> <p>d) Enters the same data with box #, printed name, date, time and signature here on IW1's script:</p> <p>Box # <u>1261</u></p> <p>Printed Name <u>Gaurab Upadhaya</u></p> <p>Date <u>16 Jun 2010</u></p> <p>Time <u>1743</u></p> <p>Signature <u>[Signature]</u></p>	FA	17:43

**Hand out key to CO7**

Step	Activity	Initial	Time
14	<p>CO7:</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</p>		