ICANN DNSSEC Key Ceremony Scripts

Abbreviations

TEB = Tamper Evident Bag (MMF Industries, item #2362010N20 small or #2362011N20 large)
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller
MC= Master of Ceremonies

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	Bert Smith	12 Jul 2010	18:00 UTC
MC	Richard Lamb /US		13JUL2010	1:53
CA	Mehmet Akcin /US		13 July 10	1:55
IW1	Francisco Arias /MX		13-JUL/2010	1:52
IW2	Kim Davies /AU		13 JULY 2010	0146
IW3	David Closson/ US		13 July 2010	01:49
SA1	Reed Quinn /US		13 July 2010	01:46
SA2	Jesse Samora /US	Not present	FA	
SSC1	Anand Mishra /US		13 July 2010	1:48
SSC2	Geoff Bickers/US		13 JULY 2010	1:49
CO1	Masato Minda /JP		13 July 2010	01 48
CO2	Dmitry Burkov /RU		13 July 2010	1:49
CO3	Joao Damas /PT		13 July 2010	1:47
CO4	Carlos Martinez /UY		13 Jul 10	1 45
CO5	Edward Lewis /US		13 Jul 10	1:57
CO6	Andy Linton /NZ		13 Jul 10	1:47
CO7	Subramanian Moonesamy /MU		13 JUL 2010	1:49
Backup CO	Christopher Griffiths / US		13 Jul 10	01:48
EW1	Duane Wessels /US		13 Jul 10	0147
EW2	Ken Michaels /US ~~Or Cara Beston /US~~		13 JUL 10	1:50
EW3	Jakob Schlyter /SE		13 Jul 10	1:45
EW4	Fredrik Ljunggren /SE		13 Jul 10	1:45

Title	Printed Name/Citizenship	Signature	Date	Time
EW5	Ondrej Filip / CZ		17 JUL	1150
EW6	Steve Conte/US	Not present	FA	
EW6	David Conrad/US		2010-7-13	1:52
Backup CA	Joe Abley		2010-07-13	0151
EW	Cara Beston		7/13/10	1:50

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. 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	CAs, SAs or IWs escort participants into the Ceremony Room.	FA	20:16

Sign into Key Ceremony Room

Step	Activity	Initial	Time
2	CAs, SAs or IWs have all participants sign into the Ceremony Room log.	FA	20:16

Emergency Evacuation Procedures

Step	Activity	Initial	Time
3	CA or MC review emergency evacuation procedures with participants.	FA	20:16

Verify Time and Date

Step	Activity	Initial	Time
4	IW1 enters date (month/day/year), UTC time using a reasonably accurate (may consult participants) wall clock visible to all here: Date (UTC): 12 July 2010 Time (UTC): 20:17 All entries into this script or any logs should follow this common source of time.	FA	20:17

Open Credential Safe #2

Step	Activity	Initial	Time
5	CA and IW1 escort SSC2 and COs 1 through 4 into the safe room together.	FA	20:18

Step	Activity	Initial	Time
6	SSC2, while shielding combination from camera, opens Safe #2.	FA	20:22
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	20:23

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

Hand out key to CO1

Step	Activity	Initial	Time
8	CO1: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and signature here on IW1's script: Box # 1788 Printed Name Masato Minda Date 12 JUL 2010 Time 20:25 Signature 民田雅人	FA	20:26

Hand out key to CO2

Step	Activity	Initial	Time
9	CO2: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and	Next	Page

Step	Activity	Initial	Time
	signature here on IW1's script: Box # 1789 Printed Name Dmitry Burkov Date 12.07.2010 Time 20:28 Signature	FA	20:29

Hand out key to CO3

Step	Activity	Initial	Time
10	CO3: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and signature here on IW1's script: Box # 1071 Printed Name Joao Damas Date 12 JULY 2010 Time 20:30 Signature	FA	20:31

Hand out key to CO4

Step	Activity	Initial	Time
11	CO4: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and signature here on IW1's script: Box # 1068 Printed Name Carlos Martinez Date 12 / July 2010 Time 20:32 Signature Carlos Martinez	FA	20:33

Close Credential Safe #2

Step	Activity	Initial	Time
12	Once all safe deposit boxes are closed, 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.	FA	20:34
13	SSC2 places safe log back in Safe #2.	FA	20:35
14	SSC2 closes and locks Safe #2.	FA	20:35
15	CA and IW1 verify that the safe is locked and card reader indicator is green.	FA	20:35
16	IW1, CA, SSC2, and COs leave safe room closing the door behind them.	FA	20.35

Open Credential Safe #2

Step	Activity	Initial	Time
17	After a one (1) minute delay, CA and IW1 escort SSC2 and COs 5 through 7 into the safe room together.	FA	20:37
18	SSC2, while shielding combination from camera, opens Safe #2.	FA	20:42
19	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	20:43

Hand out key to CO5

Step	Activity	Initial	Time
20	CO5: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and signature here on IW1's script: Box # 1790 Printed Name Edward Lewis Date 12 July 2010 Time 20:45 Signature	FIA	20:45

Hand out key to CO6

Step	Activity	Initial	Time
21	CO6: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and signature here on IW1's script: Box # 1070 Printed Name Andy Linton Date 12 July 2010	FIA	20:47

Step	Activity	Initial	Time
	Time 2046 Signature	Prav	Page

Hand out key to CO7

Step	Activity	Initial	Time
22	CO7: a) With the assistance of CA (and his/her common key), opens the safe deposit box using one of the keys already in place and reads out box number. CO looks into the box with a flashlight to verify that the box is empty. 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. c) Makes an entry in safe log with box #, printed name, date, time and signature. IW1 initials this entry. d) Enters the same data with box #, printed name, date, time and signature here on IW1's script: Box # 1792 Printed Name Subramanian Moonesamy Date 12 July 2010 Time 20:48 Signature	FA	20:49

Close Credential Safe #2

Step	Activity	Initial	Time
23	Once all safe deposit boxes are closed, 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.	FA	20:49
24	SSC2 places safe log back in Safe #2.	FA	20:49
25	SSC2 closes and locks Safe #2.	FA	20:49
26	CA and IW1 verify that the safe is locked and card reader indicator is green.	FA	20:50
27	IW1, CA, SSC2, and COs leave safe room closing the door behind them.	FA	20:50

Open Equipment Safe #1 (Approximately 3 minutes)

Step	Activity	Initial	Time
28	After a one (1) minute delay, CA, IW1 and SSC1 enter the safe room with an empty equipment cart.	FA	20:52
29	SSC1, while shielding combination from camera, opens Safe #1.	FA	20:53
30	SSC1 takes out safe log and prints name, date, time, signature and reason (i.e., "opened safe) in safe log. IW1 initials this entry.	FA	20:54

Remove Equipment from Safe #1

Step	Activity	Initial	Time
31	CA **CAREFULLY** removes HSM1 (in TEB) from the safe and completes the next entry in the safe log indicating "HSM1 Removal," TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry.	FA	20:55
32	CA **CAREFULLY** removes HSM2 (in TEB) from the safe and completes the next entry in the safe log indicating "HSM2 Removal," TEB # and serial number, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry.	FA	20:56
33	CA takes out the TEB with the O/S DVDs from the safe and completes the next entry in the safe log indicating "DVD Removal," TEB #, printed name, date, time, and signature. CA places the item on the equipment cart. IW1 initials this entry.	FA	20:57
34	CA takes out the TEB with laptop #0 from the safe and completes the next entry in the safe log indicating "Laptop Removal", TEB #, serial number if available, printed name, date, time, and signature. CA places item on equipment cart. IW1 initials this entry.	FA	20:58
35	CA takes out TEB with West Coast SMK 1 of 4 from the safe, reads out TEB # and completes the next entry in the safe log indicating "WC SMK 1 of 4 Removal," TEB #, printed name, date, time, and signature. CA places item on equipment cart. IW1 initials this entry.	FA	20:59
36	CA takes out TEB with West Coast SMK 2 of 4 from the safe, reads out TEB # and completes the next entry in the safe log indicating "WC SMK 2 of 4 Removal," TEB #, printed name, date, time, and signature. CA places item on equipment cart. IW1 initials this entry.	FA	21:00
37	CA takes out TEB with West Coast SMK 3 of 4 from the safe, reads out TEB # and completes the next entry in the safe log indicating "WC SMK 3 of 4 Removal," TEB #, printed name, date, time, and signature. CA places item on equipment cart. IW1 initials this entry.	FA	21:01
38	CA takes out TEB with West Coast SMK 4 of 4 from the safe, reads out TEB # and completes the next entry in the safe log indicating "WC SMK 4 of 4 Removal," TEB #, printed name, date, time, and signature. CA places item on equipment cart. IW1 initials this entry.	FA	21:01

Step	Activity	Initial	Time
39	CA takes out TEB with West Coast Application Key and HSMFD bundle from the safe, reads out TEB # and completes the next entry in the safe log indicating "WC APP Key and HSMFD Removal," TEB #, printed name, date, time, and signature. CA places item on equipment cart. IW1 initials this entry.	FA	21:02
40	CA removes any power supply units, USB port expander, USB serial adaptor, smartcards, blank HSMFDs, cables and other equipment necessary for HSMs and laptop from safe and places them on the equipment cart. No log entry is necessary.	FA	21:04

Close Equipment Safe #1

Step	Activity	Initial	Time
41	SSC1 makes an entry including printed name, date, time and signature into the safe log indicating "closing of the safe". IW1 initials this entry.	FA	21:05
42	SSC1 places safe log back in safe.	FA	21:05
43	SSC1 closes and locks Safe #1.	FA	21:05
44	CA and IW1 verify that the safe is locked.	FA	21:05

Roll Equipment into Ceremony Room

Step	Activity	Initial	Time
45	CA, SSC1, IW1 and equipment cart leave the safe room, closing the entry to the safe room securely behind them.	FA	21:06

Initialization Script for AEP Keyper 2.0

Set Up Laptop

Step	Activity	Initial	Time
46	CA inspects the O/S DVD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior script entry. IW1 enters the TEB # below. TEB # A1300 4301	FA	21:08
47	CA inspects the laptop TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior script entry. IW1 enters the TEB # and serial # below. TEB # A2734917 Serial # 372401477333	FA	21:09
48	CA takes O/S DVDs and laptop out of TEBs placing them on key ceremony table; discards TEBs; connects laptop power, external display, printer and boots laptop from a DVD.	FA	21:14

Step	Activity	Initial	Time
49	CA presses "CTRL+ALT+F2" to get a console prompt and logs in as root.	FA	21:16
50	CA enters the commands **`system-config-display --noui`** and **`killall Xorg`** CA ensures that external display works.	FA	21:17
51	CA logs in as root	FA	21:17
52	CA configures printer as default and prints test page.	FA	21:18
53	CA opens a terminal window and maximizes its size for visibility.	FA	21:19
54	CA checks and fixes date and time on laptop based on wall clock ensuring the correct time zone has been chosen.	FA	21:20
55	CA inserts USB port expander into laptop.	FA	21:20
56	CA inspects the West Coast Application Key and HSMFD TEB for tamper evidence; reads out TEB # while IW1 observes and matches it to the prior key ceremony script entry. IW1 enters the TEB # below. TEB # A 14377113	FA	21:22
57	CA carefully opens above TEB and removes HSMFDs from TEB, plugs one of them into free USB slot on the laptop – not expander and waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes pop up FD window.	FA	21:23
58	CA removes the two Application Key backup cards and places them in the card holder visible to camera. CA discards TEB.	FA	21:24

Start Logging Terminal Session

Step	Activity	Initial	Time
59	CA changes the default directory to the HSMFD by executing **`cd /media/HSMFD`**	FA	21:24
60	CA executes **`script script-20100712.log`** to start a capture of terminal output.	FA	21:24

Start Logging HSM Output

Step	Activity	Initial	Time
61	CA connects two (2) serial to USB null modem cables to laptop. Please note that the first USB cable connected will be "ttyUSB0", the second will be "ttyUSB1".	FA	21:25
62	CA opens a second terminal screen and executes **`cd /media/HSMFD`** and executes **`ttyaudit /dev/ttyUSB0 /dev/ttyUSB1`** to start logging HSM serial port outputs. Note: DO NOT unplug USBs from	FA	21:26

Step	Activity	Initial	Time
	laptop as this causes logging to stop.	Prev.	page

Initializing HSM1

Step	Activity	Initial	Time
63	CA inspects the HSM1 TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it to the prior Acceptance script entry. IW1 enters TEB # and serial # below. TEB # ~~A22~~A2734918 / Serial # K6002020	FA	21:27
64	CA removes HSM1 from TEB; discards TEB and plugs ttyUSB0 null modem serial cable to the back.	FA	21:28
65	CA connects power to HSM. Status information should appear on the serial logging screen and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state. IW1 matches displayed HSM serial number with above.	FA	21:37

Making Security Officer (SO) Cards (Approximately 10 minutes)

Step	Activity	Initial	Time
66	CA makes two (2) sets of the seven (7) Security Officer (SO) cards via "Issue Cards" from main menu (use '>' key to navigate menu) with "num req cards" equal 3 and total number "num cards" equal 7 using pre-labeled cards. Note: Default PIN="11223344". As each card is created the CA shows it to the participants and places it in the card holder visible to the camera.	FA	21:44

Going Operational and Setup (Approximately 10 minutes)

Step	Activity	Initial	Time
67	CA sets the HSM operational ("Go Operational" on menu) using three (3) of a set of SO cards. When presented with "Import config" press CLR button repeatedly until the "Set Online" menu item is reached. HSM date and time are not used in the ceremony. List cards used and order here (e.g., 2 of 7, 5 of 7...) ____1____ of 7, ____2____of 7, ____3_____of 7, all from Set #____1____	FA	21:46
68	CA then dumps the status of the HSM using the "Output Status" menu item (using '>' key).	FA	21:46
69	Using `less ttyaudit-ttyUSB0-20100712-*.log` or scrolling, the CA verifies settings below. **Global Key Export Enabled** **App Key Import Disabled** **App Key Export Disabled** **Asymmetric Key Gen Enabled** **Symmetric Key Gen Enabled**	Next page	

Step	Activity	Initial	Time
	Symmetric Key Derive Disabled **Signing Enabled** **Signature Verification Enabled** **MAC Gen Enabled** **MAC Ver Enabled** **Enc/Dec Enabled** **Delete Asym Key Enabled** **Delete Sym Key Enabled** **Output Key Details Enabled** **Output Key Summary Enabled** **Suite B Algorithms Enabled** **Non Suite B Algorithms Enabled** **AES SMK** **Auto Online Disabled** **FIPS Mode** Note: for auto online disable, use HSM Mgmt menu	FA	21:51
70	If settings do not match, CA fixes the settings with three (3) of a set of SO cards using "API Setting" via "Key Mgmt" (e.g., if LCD display shows "key import disable" this means key import is enabled. Click ENT to disable.) List cards used and order here (e.g., 2 of 7, 5 of 7...) ____4____ of 7, ____5____of 7, _____6_____of 7, all from Set #___1____	FA	21:51
71	CA checks settings by dumping the status of the HSM using the "Output Status" menu item (using '>' key).	FA	21:51

Making AAK (Adapter Authorization Key) Backup Cards

Step	Activity	Initial	Time
72	CA makes one set of two (2) AAK backup cards using pre-labeled cards and using three (3) of a set of SO cards via the "Key Mgmt", "AAK", "Backup" menu items. CA presses CLR when done. As each card is created the CA shows it to the participants and places it in the card holder visible to the camera. List cards used and order here (e.g., 2 of 7, 5 of 7...) ____7____ of 7, ____1____of 7, ____2_____of 7, all from Set #___1_____	FA	21:54

Importing the SMK (Approximately 5 minutes)

Step	Activity	Initial	Time
73	CA inspects the West Coast SMK 1 of 4 for tamper evidence; reads out TEB # while IW1 observes and matches it with the prior key ceremony script entry. CA opens TEB and places it in card holder visible to camera. IW1 enters the TEB # below. CA discards TEB. TEB # A14377095	FA	21:55
74	CA inspects the West Coast SMK 2 of 4 for tamper evidence; reads out TEB # while IW1 observes and matches it with the prior key ceremony script entry. CA opens TEB and places it in card holder visible to camera. IW1	Next	Page

Step	Activity	Initial	Time
	enters the TEB # below. CA discards TEB. TEB # A14377096	FA	21:57
75	CA inspects the West Coast SMK 3 of 4 for tamper evidence; reads out TEB # while IW1 observes and matches it with the prior key ceremony script entry. CA opens TEB and places it in card holder visible to camera. IW1 enters the TEB # below. CA discards TEB. TEB # A14377094	FA	21:57
76	CA inspects the West Coast SMK 4 of 4 for tamper evidence; reads out TEB # while IW1 observes and matches it with the prior key ceremony script entry. CA opens TEB and places it in card holder visible to camera. IW1 enters the TEB # below. CA discards TEB. TEB # A14377097	FA	21:58
77	CA imports SMK using any 2 of the 4 SMK cards that were generated for the West Coast Facility initialization and three (3) of a set of SO cards via the "Key Mgmt", "SMK", "Restore" menu item. List cards used and order here (e.g., 2 of 7, 5 of 7...) SMKs: 1, 2 ___1___ of 7, ___2___ of 7, ___3___ of 7, all from Set #___2___	FA	22:02

Backing up Key into HSM1

Step	Activity	Initial	Time
78	CA imports the new KSK using three (3) of a set of SO cards (if necessary) via the "Key Mgmt", "App Keys", "Restore" menu items and inserting one of the West Coast Application Key backup smart cards. When prompted for a second card, press CLR. List cards used and order here (e.g., 2 of 7, 5 of 7...) App 1 of 1, set 4 ___4___ of 7, ___5___ of 7, ___6___ of 7, all from Set #___2___	FA	22:03

Making Operator (OP) Cards

Step	Activity	Initial	Time
79	CA makes one set of the seven (7) Operator (OP) cards using pre-labeled smartcards with number needed (num req cards) equal 3 and total number (num cards) equal 7 using three (3) of a set of SO cards via the "HSM Mgmt" menu and "Issue Cards". CA presses CLR key to return to main menu. Note: Default PIN="11223344". As each card is created the CA shows it to the participants and places it in the card holder visible to the camera. List cards used and order here (e.g., 2 of 7, 5 of 7...) 1 X X of 7, ___X X 7 of 7, ___X 6 of 7, all from Set #___2___	FA	22:11

mA

Enable/Activate HSM1

Step	Activity	Initial	Time
80	CA sets HSM1 online ("Set Online" menu item) using three (3) OP cards. The "Ready" LED should go on. List cards used and order here (e.g., 2 of 7, 5 of 7...) _____1_____ of 7, _____2_____ of 7, _____3_____ of 7	FA	22:12

Check Network between Laptop and HSM1

Step	Activity	Initial	Time
81	CA connects HSM to laptop using Ethernet cable.	FA	22:13
82	CA tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` on the laptop terminal window and looking for responses. Ctrl-C to exit program. Switch back to ttyaudit screen when done.	FA	22:13
83	CA disconnects Ethernet cable from back of HSM.	FA	22:13

Initializing HSM2

Step	Activity	Initial	Time
84	CA inspects the HSM2 TEB for tamper evidence; reads out TEB # and serial # while IW1 observes and matches it with the prior Acceptance script entry. IW1 enters TEB # and serial # below. TEB # A27349 19 / Serial # K6002018	FA	22:16
85	CA removes HSM2 from TEB; discards TEB and plugs the remaining null modem serial cable to the back.	FA	22:16
86	CA connects power to HSM. Status information should appear on the serial logging screen and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state. IW1 matches displayed HSM serial number with above.	FA	22:19

Importing the AAK

Step	Activity	Initial	Time
87	CA imports AAK using the HSM main menu "Restore AAK" and AAK cards. Once imported, press CLR.	FA	22:20

Going Operational and Setup

Step	Activity	Initial	Time
88	CA sets the HSM operational ("Go Operational" on menu) using three (3) of a set of SO cards. When presented with "Import config" press CLR button repeatedly until you reach the "Set Online" menu item. List cards used and order here. ____1____ of 7, ____2____of 7, ____3____of 7, all from Set #____1____	FA	22:22

Step	Activity	Initial	Time
89	CA then dumps the status of the HSM via the "Output Status" menu item (using '>' key).	FA	22:22
90	Using **`less ttyaudit-ttyUSB1-20100712-*.log`** or scrolling, the CA verifies settings below. **`Global Key Export Enabled`** **`App Key Import Disabled`** **`App Key Export Disabled`** **`Asymmetric Key Gen Enabled`** **`Symmetric Key Gen Enabled`** **`Symmetric Key Derive Disabled`** **`Signing Enabled`** **`Signature Verification Enabled`** **`MAC Gen Enabled`** **`MAC Ver Enabled`** **`Enc/Dec Enabled`** **`Delete Asym Key Enabled`** **`Delete Sym Key Enabled`** **`Output Key Details Enabled`** **`Output Key Summary Enabled`** **`Suite B Algorithms Enabled`** **`Non Suite B Algorithms Enabled`** **`AES SMK`** **`Auto Online Disabled`** **`FIPS Mode`** Note: for auto online disable, use HSM Mgmt menu	FA	22:26
91	If the settings do not match, CA fixes the settings with three (3) of a set of SO cards using "API Setting" via "Key Mgmt" (e.g., if LCD display shows "key import disable" this means key import is enabled. Click ENT to disable.) List cards used and order here (e.g., 2 of 7, 5 of 7...) MP ___1___ of 7, ___2___ of 7, ___3___ of 7, all from Set #___1___	FA	22:26
92	CA checks settings by dumping the status of the HSM using the "Output Status" menu item (using '>' key).	FA	22:26

Destroying the AAK cards

Step	Activity	Initial	Time
93	CA erases the two AAK cards using three (3) of a set of SO cards via "Key Mgmt", "AAK", "Clear Card", "# Cards" menu items. After ensuring that the shredder is not plugged into the same outlet as the HSMs, CA shreds cards. List cards used and order here (e.g., 2 of 7, 5 of 7...) MP ___1___ of 7, ___2___ of 7, ___3___ of 7, all from Set #___1___	FA	22:30

Importing the SMK (Approximately 5 minutes)

Step	Activity	Initial	Time
94	CA imports SMK using any 2 of the 4 SMK cards that were generated for the West Coast Facility initialization and three (3) of a set of SO cards via the "Key Mgmt", "SMK", "Restore" menu item. List cards used and order here (e.g., 2 of 7, 5 of 7...) SMK: 1, 4 ____1____ of 7, ____2____of 7, ____3____of 7, all from Set #____2____	FA	22:32

Backing up Key into HSM2

Step	Activity	Initial	Time
95	CA imports the new KSK using three (3) of a set of SO cards (if necessary) via the "Key Mgmt", "App Keys", "Restore" menu items and inserting one of the West Coast Application Key backup smart cards. When prompted for a second card, press CLR. App Key 3 ____4____ of 7, ____5____of 7, ____6____of 7, all from Set #____2____	FA	22:33

Testing HSM2

Step	Activity	Initial	Time
96	CA sets HSM online ("Set Online" menu item) using three (3) OP cards. The "Ready" LED should go on. List cards used and order. (e.g., 2 of 7, 5 of 7...) ____~~4~~ 5____ of 7, ____~~5~~ 6____ of 7, ____~~6~~ 7____ of 7	FA	22:35
97	CA connects HSM to laptop using Ethernet cable that was previously connected to HSM1.	FA	22:35
98	CA tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` on the laptop terminal window. Control-C to exit program. Switch back to ttyaudit screen when done.	FA	22:36

KSR Signer Script

Insert Copy of KSR to be Signed

Step	Activity	Initial	Time
99	CA plugs FD labeled "KSR" with KSR to be signed into the laptop and waits for the O/S to recognize the FD. CA or MC points out the KSR file to be signed.	FA	22:42

Sign it with our KSK

Step	Activity	Initial	Time
100	CA identifies the KSR to be signed and runs, in the terminal window `ksrsigner Kjqmt7v /media/KSR/ksr-root-2010-q4-1.xml`	FA	22:48

Final Verification of the Hash (validity) of the KSR

Step	Activity	Initial	Time
101	When the program requests verification of the KSR hash, CA asks the Root Zone Maintainer (RZM) representative to identify themselves, present identification document for IW1 to retain and read out the SHA256 hash in PGP wordlist format for the KSR previously sent ICANN. IW1 enters RZM representative's name here: Duane Wessels	FA	22:48
102	Participants match the hash read out with that displayed on the terminal. CA asks "are there are any objections"?	FA	22:49
103	CA then enters "y" in response to "is this correct y/n?" to complete KSR signing operation. Sample output should look like Figure 1. The signed KSR (SKR) will be found in **`/media/KSR/skr-root-2010-q4-1.xml`**	FA	22:49

```
$ ksrsigner K19324 ksr-root-2010-q4-1.xml

Starting: ksrsigner K19324 ksr-root-2010-q4-1.xml (at Thu Jul 8 15:02:52 2010 PST)
Use HSM ./aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y
HSM ./aep.hsmconfig activated.
PKCS11_LIBRARY_PATH=/u2/home/lamb/dnssec/ksr/AEP/pkcs11.GCC4.0.2.so.4.07
Found 4 slots on HSM /u2/home/lamb/dnssec/ksr/AEP/pkcs11.GCC4.0.2.so.4.07
Include HSM slot 0 ? (Y/n): n
HSM slot 0 NOT included
Include HSM slot 1 ? (Y/n): n
HSM slot 1 NOT included
Include HSM slot 2 ? (Y/n): y
HSM slot 2 included
Loaded /u2/home/lamb/dnssec/ksr/AEP/pkcs11.GCC4.0.2.so.4.07 Slot=2
HSM Information:
    Label:           OtherKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper Pro 0405
    Serial:          K0705020

Include HSM slot 3 ? (Y/n): n
HSM slot 3 NOT included
Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-07-01T00:00:00 2010-07-15T23:59:59  55138,41248   19324
2  2010-07-11T00:00:00 2010-07-25T23:59:59  41248         19324
3  2010-07-21T00:00:00 2010-08-04T23:59:59  41248         19324
4  2010-07-31T00:00:00 2010-08-14T23:59:59  41248         19324
5  2010-08-10T00:00:00 2010-08-24T23:59:59  41248         19324
6  2010-08-20T00:00:00 2010-09-03T23:59:59  41248         19324
7  2010-08-30T00:00:00 2010-09-13T23:59:59  41248         19324
8  2010-09-09T00:00:00 2010-09-24T00:00:00  41248         19324
9  2010-09-20T00:00:00 2010-10-05T23:59:59  12345,41248   19324
...VALIDATED.

Validate and Process KSR ksr-root-2010-q4-1.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  12345,41248
2  2010-10-11T00:00:00 2010-10-25T23:59:59  12345
3  2010-10-21T00:00:00 2010-11-04T23:59:59  12345
4  2010-10-31T00:00:00 2010-11-14T23:59:59  12345
5  2010-11-10T00:00:00 2010-11-24T23:59:59  12345
6  2010-11-20T00:00:00 2010-12-04T23:59:59  12345
7  2010-11-30T00:00:00 2010-12-14T23:59:59  12345
8  2010-12-10T00:00:00 2010-12-25T00:00:00  12345
9  2010-12-21T00:00:00 2011-01-05T23:59:59  21639,12345
...PASSED.

SHA256 hash of KSR:
BA6388FA33FC2BE29859280A63FF9C73D308589AD613C91944951966EEF11A08F
>> shadow Galveston newborn whimsical chisel Wilmington briefcase tomorrow printer examine breadline Apollo
flatfoot Yucatan python hurricane stapler antenna endorse newsletter stockman barbecue spearhead bottomless
crumpled Montana bedlamp headwaters uncut Babylon ragtime midsummer <<

Is this correct (y/N)? y

Generated new SKR in ./skr-root-2010-q4-1.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  12345,41248   19324
2  2010-10-11T00:00:00 2010-10-25T23:59:59  12345         19324
3  2010-10-21T00:00:00 2010-11-04T23:59:59  12345         19324
4  2010-10-31T00:00:00 2010-11-14T23:59:59  12345         19324
5  2010-11-10T00:00:00 2010-11-24T23:59:59  12345         19324
6  2010-11-20T00:00:00 2010-12-04T23:59:59  12345         19324
7  2010-11-30T00:00:00 2010-12-14T23:59:59  12345         19324
8  2010-12-10T00:00:00 2010-12-25T00:00:00  12345         19324
9  2010-12-21T00:00:00 2011-01-05T23:59:59  12345,21639   19324

SHA256 hash of SKR:
E80722B215EF0B7882C056F9C0AD4CD6E610077B2EB7496837A51D27D765825A
>> trauma amusement blockade pioneer backfield unravel alone indigo miser recipe egghead Waterloo slowdown
perceptive drainage speculate tracker autopsy ahead inferno buzzard processor deckhand gravity clamshell
paperweight Belfast celebrate stopwatch glossary miser existence <<
Unloaded /u2/home/lamb/dnssec/ksr/AEP/pkcs11.GCC4.0.2.so.4.07 Slot=2

********** Log output in ./ksrsigner-20100708-220252.log **********
```

Figure 1

Print Copies of the Operation for Participants

Step	Activity	Initial	Time
104	CA prints out a sufficient number of copies for participants using **`printlog ksrsigner-20100712-*.log 30`** (this example generates 30 copies) and hands copies to participants.		22:55
105	IW1 attaches a copy to his/her script.		22:55

Backup Newly Created SKR

Step	Activity	Initial	Time
106	CA copies the contents of the KSR FD by running **`cp -p /media/KSR/* .`** for posting back to RZM.	FA	22:52
107	CA lists contents of KSR FD which should now have an SKR by running **`ls -t /media/KSR`** and then unmounts the KSR FD using **`umount /media/KSR`**	FA	22:53
108	CA removes **KSR** FD containing SKR and gives it to the RZM representative.	FA	22:53

Destroying West Coast SMK cards

Step	Activity	Initial	Time
109	CA erases the 4 (four) SMK cards using three (3) of a set of SO cards via "Key Mgmt", "SMK", "Clear Card", "num cards" =4 menu items and inserting SMK cards as prompted. After ensuring that the shredder is not plugged into the same outlet as the HSMs, CA shreds cards. List SO cards used and order here (e.g., 2 of 7, 5 of 7...) __1__ of 7, __2__ of 7, __4__ of 7, all from Set #__2__.	FA	23:00

Epilogue Script

Returning HSM1 to a TEB

Step	Activity	Initial	Time
110	CA presses RESTART button on HSM 1 and waits for self test to complete.	FA	23:49
111	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals. CA indicates "HSM 1" on TEB.	FA	23:52
112	CA reads out TEB # and HSM serial #, shows item to participants and IW1 records TEB # and HSM serial # here. TEB # A28267 32 /HSM serial # K6002020	FA	23:52

Step	Activity	Initial	Time
113	CA places item on equipment cart.	FA	23:52

Returning HSM2 to a TEB

Step	Activity	Initial	Time
114	If needed, CA presses RESTART button on HSM 2 and waits for self test to complete.	FA	23:53
115	CA disconnects HSM from power and laptop (serial and Ethernet) if connected, placing HSM into a new TEB and seals. CA indicates "HSM 2" on TEB.	FA	23:55
116	CA reads out TEB # and HSM serial #, shows item to participants and IW1 records TEB # and HSM serial # here. TEB # A2826731 /HSM serial # K6002018	FA	23:55
117	CA places item on equipment cart.	FA	23:55

Stop Recording Serial Port Activity

Step	Activity	Initial	Time
118	CA terminates HSM serial output capture by disconnecting both USB serial adaptors from laptop. CA then exits out of serial output terminal window.	FA	23:56

Stop Logging Terminal Output

Step	Activity	Initial	Time
119	CA stops logging terminal output by entering "exit" in terminal window	FA	23:57

Backup HSM FD Contents (Approximately 10 minutes)

Step	Activity	Initial	Time
120	CA displays contents of HSMFD by executing `ls -t`	FA	23:57
121	CA plugs a blank FD labeled HSMFD into the laptop, then waits for it to be recognized by the O/S (as HSMFD_); and copies the contents of the HSMFD to the blank drive for backup by executing `cp -Rp * /media/HSMFD_`	FA	13 July 2010 00:00
122	CA displays contents of HSMFD_ by executing `ls -t /media/HSMFD_`	FA	00:00
123	CA unmounts new FD using `umount /media/HSMFD_`	FA	00:00
124	CA removes HSMFD_ and places on table	FA	00:01
125	CA repeats steps 121-123	FA	00:01
126	CA repeats steps 121-123	FA	00:02
127	CA repeats steps 121-123	FA	00:03

Returning HSM FD to a TEB

Step	Activity	Initial	Time

128	CA unmounts HSMFD by executing
	`cd /tmp`
	then
	`umount /media/HSMFD`
		FA	00:04

129	CA removes HSMFD and places it and one of the backup HSMFD_ from above in new TEB; writes date, time and "HSMFD" in amount field; and seals; reads out TEB #; shows item to participants and IW1 records TEB # here TEB # A13004297 and places TEB on equipment cart.	FA	00:06

Packaging Application Key Backups

Step	Activity	Initial	Time
130	CA places the remaining original West Coast HSMFD and two Application Key cards in a TEB and seals.	FA	00:07
131	CA reads out TEB #; shows item to participants and places item on equipment cart destined for Safe #1. IW1 records TEB # here. TEB # A13004296	FA	00:08
132	Remaining HSMFDs are distributed to IW1, CA and MC to post SKR to RZM, and to review, analyze and improve on procedures.	~~FA~~ See exceptions	

Returning O/S DVD to a TEB

Step	Activity	Initial	Time
133	After all print jobs are complete, CA executes `shutdown -hP now` removes DVD and turns off laptop.	FA	0:16
134	CA places both DVDs in new TEB and seals; reads out TEB #; shows item to participants and IW1 records TEB # here. TEB # A13004332	FA	0:27
135	CA places item on equipment cart.	FA	0:27

Returning Laptop to a TEB

Step	Activity	Initial	Time
136	CA disconnects printer, display, power, and any other connections from laptop and puts laptop in new TEB and seals (indicating "Laptop #0" on TEB); reads out TEB #, serial #, laptop # and shows item to participants and IW1 records TEB #, serial # and laptop # here.	Next page	

Step	Activity	Initial	Time
	TEB # A 2826730 Serial # 372401497373 Laptop # Ø	FA	0:23
137	CA places item on equipment cart.	FA	0:23

Returning Power Supplies, USB Expander and Cables to Cart

Step	Activity	Initial	Time
138	CA places HSM and laptop power supplies, USB expander, USB serial adaptor(s), power and networking cables on equipment cart.	FA	0:29

Returning OP/SO Smartcards to TEBs

Step	Activity	Initial	Time
139	CA calls a CO1 to the front of the room (to stand behind CA). a) CA takes one (1) TEB and reads out the number while showing the bag and number to IW1 and CO. b) CA places one (1) OP card into TEB. c) CA writes down description (e.g., "OP 1 of 7" on "amount" line), initials (on "prepared by" line) and date on TEB. CA enters the same information on the sealing strip. See Figure 2 below for an example. d) IW1 inspects then initials TEB and sealing strip (next to CA's initials). e) CA seals TEB in front of IW1 and CO then hands sealing strip to IW1. IW1 keeps sealing strips for later inventory. f) IW1 records TEB and description in table below. g) CA places TEB on the ceremony table. h) CA takes one (1) TEB and reads out the number while showing the bag and number to IW1 and CO. i) CA drops two (2) SO cards, the same card from both sets (e.g., 1 of 7 from set 1 and 1 of 7 from set 2) into TEB. j) CA writes down description (e.g., "SO 1 of 7" on "amount" line), initials (on "prepared by" line) and date on TEB. CA enters the same information on the sealing strip. k) IW1 inspects then initials TEB and sealing strip (next to CA's initials). l) CA seals TEB in front of IW1 and CO then hands sealing strip to IW1. IW1 keeps sealing strips for later inventory. m) IW1 records TEB and description in table below. n) CA hands the TEB containing the SO cards, along with the TEB containing the OP card (which is on the ceremony table) to the CO. CO inspects and verifies TEB #s and contents and enters	FA	0:36

Step	Activity	Initial	Time
	date, time and signs for each TEB in the table below in IW1's script. IW1 initials table entry. CO returns to his/her seat with the TEBs, being careful not to poke or puncture TEBs.	Prov.	Page
140	CA repeats Step 139 for cards 2 of 7 for CO2	FA	0:40
141	CA repeats Step 139 for cards 3 of 7 for CO3	FA	0:43
142	CA repeats Step 139 for cards 4 of 7 for CO4	FA	0:47
143	CA repeats Step 139 for cards 5 of 7 for CO5	FA	0:52
144	CA repeats Step 139 for cards 6 of 7 for CO6	FA	0:55
145	CA repeats Step 139 for cards 7 of 7 for CO7	FA	0:59

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1
CO1	OP 1 of 7	A1300 4339	Masato Minda		13-Jul-10	0:36	FA
CO1	SO 1 of 7 Both Sets	A1300 4340	Masato Minda		13-Jul-10	0:36	FA
CO2	OP 2 of 7	A1300 4335	Dmitry Burkov		13-Jul-10	0:40	FA
CO2	SO 2 of 7 Both Sets	A1300 4336	Dmitry Burkov		13-Jul-10	0:40	FA
CO3	OP 3 of 7	A1300 4312	Joao Damas		13-Jul-10	0:43	FA
CO3	SO 3 of 7 Both Sets	A1300 4313	Joao Damas		13-Jul-10	0:43	FA
CO4	OP 4 of 7	A1300 4310	Carlos Martinez		13-Jul-10	0:47	FA
CO4	SO 4 of 7 Both Sets	A1300 4311	Carlos Martinez		13-Jul-10	0:47	FA
CO5	OP 5 of 7	~~A1660 8568~~	Edward Lewis		13-Jul-10	0:52	FA
CO5	SO 5 of 7 Both Sets	A1300 4326	Edward Lewis		13-Jul-10	0:52	FA
CO6	OP 6 of 7	A1660 8559	Andy Linton		13-Jul-10	0:55	FA
CO6	SO 6 of 7 Both Sets	A1660 8558	Andy Linton		13-Jul-10	0:55	FA
CO7	OP 7 of 7	A1660 8557	Subramanian Moonesamy		13-Jul-10	0:59	FA
CO7	SO 7 of 7 Both Sets	A1660 8556	Subramanian Moonesamy		13-Jul-10	0:59	FA

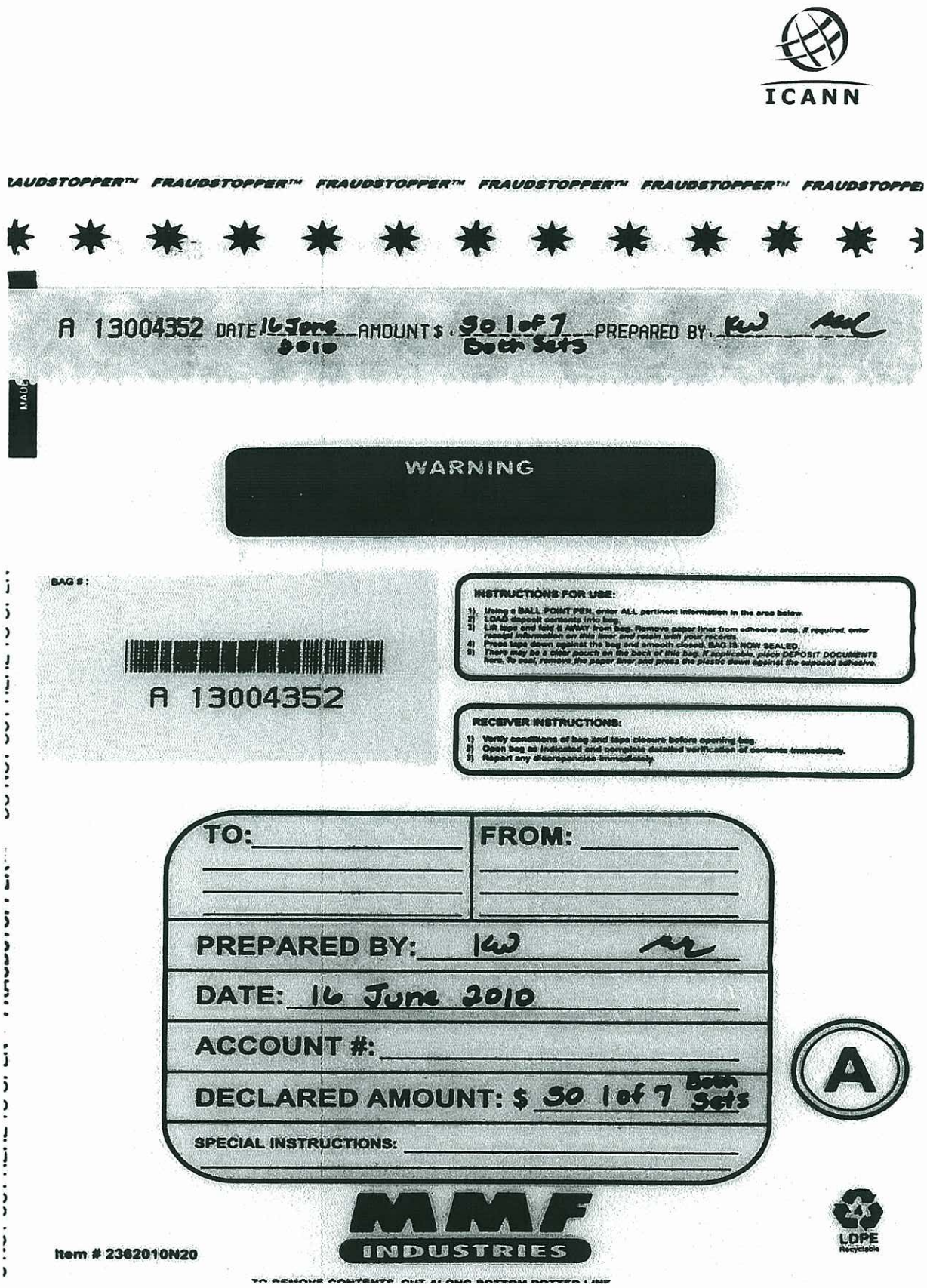

FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER™ FRAUDSTOPPER
A 13004352 DATE 16 June 2010 AMOUNT $ 30 1 of 7 Both Sets PREPARED BY KW
WARNING
BAG # :
A 13004352
INSTRUCTIONS FOR USE:
RECEIVER INSTRUCTIONS:
TO:
FROM:
PREPARED BY: KW
DATE: 16 June 2010
ACCOUNT #:
DECLARED AMOUNT: $ 30 1 of 7 Both Sets
SPECIAL INSTRUCTIONS:
A
MMF
INDUSTRIES
Item # 2362010N20
LDPE

Figure 2

Returning Equipment in TEBs to Safe #1

Step	Activity	Initial	Time
146	CA, IW1, SSC1 open safe room and enter with equipment cart.	FA	1:01
147	SSC1 opens Safe #1 shielding combination from camera.	FA	1:02
148	SSC1 removes the safe log and fills the next entry with printed name, date, time, and signature indicating "opening of the safe." IW1 initials the entry.	FA	1:03
149	CA records return of HSM1 in next entry field of safe log with TEB # and HSM1 serial #, printed name, date, time, and signature. CA **CAREFULLY** places the HSM 1 into Safe #1 and IW1 initials the entry.	FA	1:04
150	CA records return of HSM2 in next entry field of safe log with TEB # and HSM 2 serial #, printed name, date, time, and signature. CA **CAREFULLY** places the HSM2 into Safe #1 and IW1 initials the entry.	FA	1:05
151	CA records return of laptop in next entry field of safe log with TEB #, serial #, laptop #, printed name, date, time, and signature; places the laptop into Safe #1 and IW1 initials the entry.	FA	1:06
152	CA records return of HSMFDs in next entry field of safe log with TEB #, printed name, date, time, and signature; places the HSMFD into Safe #1 and IW1 initials the entry.	FA	1:07
153	CA records return of O/S DVDs in next entry field of safe log with TEB #, printed name, date, time, and signature; places the O/S DVD into Safe #1 and IW1 initials the entry.	FA	1:07
154	CA records return of the Application Key backup package in next entry field of safe log with description (e.g., App card and HSMFD), TEB #, printed name, date, time, and signature; places the TEB into Safe #1 and IW1 initials the entry.	FA	1:08
155	CA returns remaining power supplies, adaptors, USB port expander and cables to safe. No entry in log is necessary.	FA	1:09

PS

Closing Equipment Safe #1

Step	Activity	Initial	Time
156	SSC1 makes an entry including printed name, date, time, signature and notes "closing safe" in the safe log. IW1 initials the entry.	FA	1:09
157	SSC1 places log back in safe and locks Safe #1.	FA	1:10
158	IW1 and CA verify safe is locked.	FA	1:10
159	IW1, CA, and SSC1 return to ceremony room with equipment cart.	FA	1:11

Returning CO OP/SO cards to Credential Safe #2 (CO1 through CO4)

Step	Activity	Initial	Time
160	CA, IW1, SSC2, and COs 1 through 4 enter the safe room. COs bring their TEBs with them. Each CO should have 2 TEBs.	FA	1:14
161	SSC2 opens Safe #2 while shielding combination from camera.	FA	1:15
162	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating "opening of the safe." IW1 initials the entry.	FA	1:16

CO1 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
163	CO1 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:20
164	CO1 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:20
165	CO1 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:20

CO2 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
166	CO2 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:20
167	CO2 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:21
168	CO2 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:22

CO3 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
169	CO3 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:24
170	CO3 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:24
171	CO3 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:24

CO4 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
172	CO4 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:25
173	CO4 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:26
174	CO4 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:26

Closing Credential Safe #2

Step	Activity	Initial	Time
175	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "closing safe" into the safe log. IW1 initials the entry.	FA	1:27
176	SSC2 puts log back in safe and locks Safe #2.	FA	1:27
177	IW1 and CA verify safe is locked.	FA	1:28
178	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	FA	1:28

Returning CO OP/SO cards to Credential Safe #2 (CO5 through CO7)

Step	Activity	Initial	Time
179	After a one (1) minute delay, CA, IW1, SSC2, and COs 5 through 7 enter the safe room. COs bring their TEBs with them. Each CO should have 2 TEBs.	FA	1:30
180	SSC2 opens Safe #2 while shielding combination from camera.	FA	1:32
181	SSC2 removes the safe log and fills in the next entry with printed name, date, time, and signature indicating "opening of the safe" IW1 initials the entry.	FA	1:33

CO5 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
182	CO5 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:35
183	CO5 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:35
184	CO5 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:35

CO6 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
185	CO6 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:40
186	CO6 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:40
187	CO6 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:40

CO7 returns OP/SO cards to Safe #2

Step	Activity	Initial	Time
188	CO7 along with CA (using his/her common key) opens his/her respective safe deposit box and reads out box number inside Safe #2.	FA	1:43
189	CO7 makes an entry into the safe log indicating the return of OP and SO cards including Box #, TEB #s, card type, printed name, date, time, and signature. IW1 initials the entry after comparing TEB# s and card type to his/her script.	FA	1:43
190	CO7 places his/her TEBs into his/her box and locks the safe deposit box with the help of the CA.	FA	1:43

Closing Credential Safe #2

Step	Activity	Initial	Time
191	Once all safe deposit boxes are closed, SSC2 makes an entry including printed name, date, time, and signature and notes "closing safe" into the safe log. IW1 initials the entry.	FA	1:43
192	SSC2 puts log back in safe and locks Safe #2.	FA	1:44
193	IW1 and CA verify safe is locked.	FA	1:44
194	CA, IW1, SSC2, and COs leave safe room closing the door behind them making sure it is locked.	FA	1:44

Participant Signing of IW1's Script

Step	Activity	Initial	Time
195	All participants enter printed name, date, time, and signature on IW1's script coversheet.	FA	1:55
196	CA reviews IW1's script and signs it.	FA	1:58

Signing out of Ceremony Room

Step	Activity	Initial	Time
197	CA, SA or IWs ensure that all participants sign out of Ceremony Room log and are escorted out of the Ceremony Room.		

Filming Stops

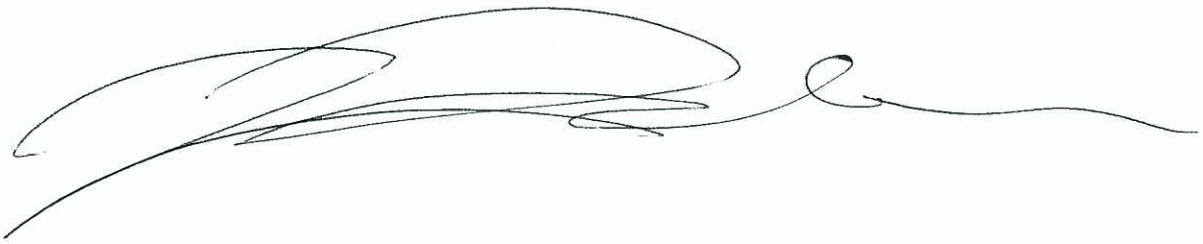
Step	Activity	Initial	Time
198	SA stops filming and makes 2 copies of film, one for on-site and one for off-site storage along with IW1 script copies made below.		

Copying and Storing the Script

Step	Activity	Initial	Time
199	IW1 makes at least 5 copies of his/her script: one for off-site storage, one for on-site storage, one for IW1, and copies for other participants, as requested.		

All remaining participants sign out of ceremony room log and leave.

Mehmet Akcin
Ceremony Administrator



Francisco Arias
Internal Witness

DESCRIPTION	TEB #
West Coast SMK 1 of 4	A14377095
West Coast SMK 2 of 4	A14377096
West Coast SMK 3 of 4	A14377094
West Coast SMK 4 of 4	A14377097
West Coast APP X2 + HSMFD X2	A14377113

VeriSign®
487 EAST MIDDLEFIELD ROAD
MOUNTAIN VIEW, CA 94043
P650 961 7500
F650 961 7300
www.VeriSign.com

July 6, 2010

To Whom It May Concern:

This is a letter of Verification of Employment for Mr. Duane Wessels. VeriSign, Inc. has employed Mr. Wessels full-time since January 11, 2010 as a Principal Engineer of Engineering R&D team.

VeriSign is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, our SSL, authentication, identity protection, and registry services allow companies and consumers all over the world to engage in trusted communications and commerce.

For over 10 years, VeriSign Internet infrastructure has been at the very heart of the Internet, enabling key transactions and protecting valuable data. VeriSign facilitates as many as 31 billion authoritative Domain Name System (DNS) queries a day, and has been providing this service since 1998 with 100% availability. Over the years the VeriSign Internet infrastructure has scaled quickly and dramatically, and has the capacity to scale just as dramatically in the coming years, as the world moves to Internet-based transactions. VeriSign SSL Certificates have provided a strong foundation for e-commerce, and the VeriSign Secured® Seal, the most recognized symbol of trust on the Internet (TNS Study, 2006), is viewed over 100 million times a day on browsers all over the world.

Should you have further questions, please do not hesitate to contact me.

Sincerely,

Susanna Wong
Human Resources Services
650-426-4842

July 12, 2010

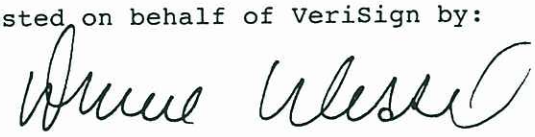
The SHA256 hash of the 2010 Q4 KSR file is:

a17e 5397 93b2 6111 12c4 f591 a06a f4fb
c222 1ddd d717 94bc 72d5 aee9 10c7 2543

The PGP wordlist for the hash above is:

ratchet insurgent dwelling mosquito playhouse pioneer fallout
babylon atlas reproduce vapor miracle ragtime hamburger upshot
wichita snapshot candidate belfast tambourine stopwatch bookseller
pluto pyramid highchair specialist robust ultimate assume retraction
bombast decimal

Attested on behalf of VeriSign by:



Duane Wessels
Principal Engineer
VeriSign, Inc.

```
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2010-q4-1.xml (at Mon Jul 12 22:44:26 2
010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper Pro 0405
    Serial:          K6002018

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-07-01T00:00:00 2010-07-15T23:59:59  55138,41248   19036
2  2010-07-11T00:00:00 2010-07-25T23:59:59  41248         19036
3  2010-07-21T00:00:00 2010-08-04T23:59:59  41248         19036
4  2010-07-31T00:00:00 2010-08-14T23:59:59  41248         19036
5  2010-08-10T00:00:00 2010-08-24T23:59:59  41248         19036
6  2010-08-20T00:00:00 2010-09-03T23:59:59  41248         19036
7  2010-08-30T00:00:00 2010-09-13T23:59:59  41248         19036
8  2010-09-09T00:00:00 2010-09-24T00:00:00  41248         19036
9  2010-09-20T00:00:00 2010-10-05T23:59:59  40288,41248   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2010-q4-1.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  40288,41248
2  2010-10-11T00:00:00 2010-10-25T23:59:59  40288
3  2010-10-21T00:00:00 2010-11-04T23:59:59  40288
4  2010-10-31T00:00:00 2010-11-14T23:59:59  40288
5  2010-11-10T00:00:00 2010-11-24T23:59:59  40288
6  2010-11-20T00:00:00 2010-12-04T23:59:59  40288
7  2010-11-30T00:00:00 2010-12-14T23:59:59  40288
8  2010-12-10T00:00:00 2010-12-25T00:00:00  40288
9  2010-12-21T00:00:00 2011-01-05T23:59:59  21639,40288
...PASSED.

SHA256 hash of KSR:
A17E539793B2611112C4F591A06AF4FBC2221DDDD71794BC72D5AEE910C72543
>> ratchet insurgent dwelling mosquito playhouse pioneer fallout Babylon atlas reproduc
e vapor miracle ragtime hamburger upshot Wichita snapshot candidate Belfast tambourine
stopwatch bookseller Pluto pyramid highchair specialist robust ultimate assume retracti
on bombast decimal <<

Generated new SKR in /media/KSR/skr-root-2010-q4-1.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2010-10-01T00:00:00 2010-10-15T23:59:59  40288,41248   19036
```

```
2  2010-10-11T00:00:00 2010-10-25T23:59:59  40288         19036
3  2010-10-21T00:00:00 2010-11-04T23:59:59  40288         19036
4  2010-10-31T00:00:00 2010-11-14T23:59:59  40288         19036
5  2010-11-10T00:00:00 2010-11-24T23:59:59  40288         19036
6  2010-11-20T00:00:00 2010-12-04T23:59:59  40288         19036
7  2010-11-30T00:00:00 2010-12-14T23:59:59  40288         19036
8  2010-12-10T00:00:00 2010-12-25T00:00:00  40288         19036
9  2010-12-21T00:00:00 2011-01-05T23:59:59  40288,21639   19036

SHA256 hash of SKR:
00CC341B7B3BAEE2E62B1AA6A58DEF07F02E4950E959E6A6ACBD7CEFF2741257
>> aardvark revolver choking bravado kickoff councilman robust tomorrow tracker Cheroke
e beehive paragon reindeer microscope uncut amusement unearth coherence deckhand embezz
le treadmill examine tracker paragon ribcage quantity kiwi unravel uproot hydraulic atl
as Eskimo <<
Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

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

1	IW notes date and time of key ceremony exception and signs here: 12 July 2010	FA	22:14
2	IW Describes exception and action below		

– We were missing a file at step 100; skr.xml
It was copied from the HSM FD to the KSR FD

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

2

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

1	IW notes date and time of key ceremony exception and signs here: 12 July 2010	FA	23:01
2	IW Describes exception and action below		

- After step 109 we took a break.
- Restarting at 23:47

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

3

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

1	IW notes date and time of key ceremony exception and signs here: 13 July 2010 @	FA	00:09
2	IW Describes exception and action below		

– It was decided to have the three remaining HSM FD backups each in one $ TEB

TEB #1: A13004309 Audit 1
TEB #2: A13004315 Audit 2
TEB #3: A13004314 East coast

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

4

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

1	IW notes date and time of key ceremony exception and signs here: 13 July 2010	FA	00:17
2	IW Describes exception and action below		

- It was requested by Ondrej (EW) to have the Hash of the OS DVD calculated with a different (to the one used during the ceremony) laptop
- while the hash was being calculated we proceed at step 136.
- Hash was matched at 0:25

– End of DNSSEC Script Exception –

ICANN DNSSEC Script Exception

5

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

1	IW notes date and time of key ceremony exception and signs here: 13 July 2010	FA	1:37
2	IW Describes exception and action below		

– Box 1070 won't open, a new box was assigned.

– New box 1072.

– End of DNSSEC Script Exception –