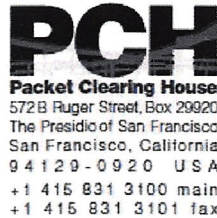






ORIGINAL




DNSSEC Key Ceremony Script Monday, November 23, 2015


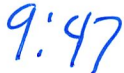
Sign In to Facility

Step	Activity	Initial	Time (PST)
1	FO has all participants sign in on Facility Sign-In Sheet before entering the Key Management Facility.		9:32
2	FO reviews emergency evacuation procedures and other relevant information with participants.		9:45
3	FO collects and stores participants' cell phones and computers outside the Key Management Facility. Cameras and other recording devices are permitted in the Key Management Facility. SC may retain and use a computer during the ceremony.		9:39
4	FO verifies the functioning of audio and video recording.		9:45


Enter the Key Management Facility

Step	Activity	Initial	Time (PST)
5	As the participants enter the Key Management Facility, the EW verifies the identity of each by examining a government-issued photo identification, notes the type and number of each piece of identification, and the participant's entry time on the Participant Signature Sheet. Participants should not sign the sheet until the end of the ceremony. As the participants are identified each is issued an identification vest.		9:42


Ground Rules

Step	Activity	Initial	Time (PST)
6	<p>CA previews ground rules and break procedures with participants.</p> <ul style="list-style-type: none">- We follow the script step by step.- Each step is read aloud by CA prior to its performance.- Upon the completion of each step, its completion and the time of completion are announced for the record, and the EW records the completion time and initials his copy of the script.- If any participant notices a problem or believes that an error has occurred, that participant should interrupt immediately, and the participants should agree upon a resolution prior to proceeding.- Any significant discrepancies or deviations from the script will be recorded by the EW on the provided Exception Sheets.- Questions and suggestions for improvement are welcome at any time, will be incorporated into the record, and contribute to the quality of this and future ceremonies.		





Verify Time and Date

Step	Activity	Initial	Time (PST)
7	<p>EW reads aloud and records the date (month/day/year) and time (UTC) using an NTP-synchronized clock visible to all. Participants verify that the time is correct.</p> <p>Date: <u>11/23/2015</u></p> <p>Time: <u>17:47</u></p> <p>While this and previous steps are recorded using local time, subsequent steps and any associated logs follow this common source of time and are recorded in UTC.</p>		9:47


Verify UPS

Step	Activity	Initial	Time (UTC)
8	<p>If there is a UPS (uninterruptible power supply), then</p> <ul style="list-style-type: none">- CA verifies that the UPS is connected to and receiving power from the electric grid and that it is charged.- CA verifies that the audio recorder is receiving power from the UPS.		17:48




Remove Equipment from Safe




Step	Activity	Initial	Time (UTC)
9	SC opens the safe and records this action as an entry in the safe's log sheet.		17:49
10	<p>SC collects the following items from the safe:</p> <ul style="list-style-type: none"> - KSK-HSM-01B-SJC HSM - boot-DVD - laptop <p>...and any other items that may be required, indicating removal of each with any applicable TEB or serial numbers in the safe's log sheet. SC also provides any necessary power supplies and cables. Equipment is placed on the work surface visible to all participants.</p> <p>If the immediately preceeding key ceremony was also held in this same facility, the HSMFD is also collected from the safe. If the preceeding key ceremony was performed in a different facility, any HSMFD from the preceeding key ceremony may be used, provided it's still in its TEB and the TEB number and integrity are verified.</p>		17:53
11	<p>CA reads out KSK-HSM-01B-SJC HSM TEB and serial numbers while EW checks that they match those recorded in the script from the most recent key ceremony performed at this site.</p> <p>TEB# A4128457</p> <p>Serial# K1011066</p>		17:54
12	<p>CA reads out boot-DVD, laptop, and HSMFD TEB numbers while EW checks that they match those recorded in the script from the most recent key ceremony performed at this site.</p> <p>DVD TEB# A28410717</p> <p>Laptop TEB# A4128458</p> <p>HSMFD TEB# A28410722 <i>A28410718</i></p>		18:01



Collect OP Cards

Step	Activity	Initial	Time (UTC)
13	CA collects OP cards from COs, reading out and comparing TEB numbers with those recorded in the most recent ceremony each participated in, reproduced for convenience in the appendices of this document. Different COs may appear on different pages. Note any discrepancies. CA places the OP cards in plain view on the work surface, removing cards from TEBs, discarding used TEBs but saving warning slips for reuse.		18:10


Set Up Laptop

Step	Activity	Initial	Time (UTC)
14	<p>CA removes the boot-DVD and laptop from their TEBs, showing participants that the laptop contains no boot devices.</p> <p>CA places the boot-DVD and the laptop on the work surface, connects laptop power to the UPS. Any external monitor or projector may be powered from either the grid (or the UPS if it's large enough).</p> <p>Power the laptop on, booting it from the DVD.</p> <p>During the boot process, make sure the output on the laptop screen is also visible on any external monitor or projector.</p> <p>Booting from the DVD may generate warnings of kernel crash, which can be ignored if it continues to boot.</p>		18:19
15	CA logs in as root.		18:21
16	CA opens a terminal window.		18:21




17	<p>CA verifies the time zone, date, and time on the laptop and synchronizes it if necessary.</p> <p>Display the current time and timezone:</p> <pre>date</pre> <p>If the timezone is not set to UTC:</p> <pre>cd /etc/ rm localtime ln -s /usr/share/zoneinfo/UTC localtime</pre> <p>Set time to match the wall clock:</p> <pre>date mmddHHMMYYYY</pre> <p>Verify:</p> <pre>date</pre>		18:24
18	<p>CA disables screen saver by typing</p> <pre>xset s off</pre> <pre>(while sleep 1800;do xset -dpms;done&)</pre> <p>Then closes the window by typing</p> <pre>exit</pre> <p>Now, using the GUI menu, in</p> <p>"System" -> "Preferences" -> "Screensaver"</p> <p>uncheck "activate screen saver when computer is idle"</p> <p>Click "Close". In</p> <p>"System" -> "Preferences" -> "More Preferences" -> "Power Management"</p> <p>Ensure both sliders in "Running on AC" are set to "never".</p> <p>Click "Close".</p>		18:26
19	<p>CA opens a terminal window, which we will refer to as the "checksum window". In this window the CA starts the calculation of the sha256 checksum of the boot-DVD. This calculation takes about 9 minutes to complete and the results will be verified in a later step; this step is considered complete as soon as the command is issued.</p> <pre>sha256sum /dev/cdrom</pre>		18:26

20	CA connects USB hub to laptop.		18:27
21	CA removes HSMFD from its TEB, connects it to the laptop, and waits for operating system to recognize the FD. CA lets participants view contents of HSMFD then closes FD window.		18:32


Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
22	CA opens a new terminal window, which we will refer to as the "command window". In this window the CA will change the default directory to the HSMFD and start capture of terminal output to a file: <code>cd /media/HSMFD</code> <code>script script-20151123.log</code>		18:33


Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
23	CA inspects the HSM TEB for evidence of tampering and removes the HSM from its TEB; discards the TEB and connects the ttyUSB0 null modem serial adaptor and cable.		18:34
24	CA connects the ttyUSB0 null modem serial adaptor and cable to the laptop, completing the serial connection between laptop and HSM.		18:35
25	CA opens a new terminal window, which we will refer to as the "ttyaudit window". In this window the CA will start logging HSM serial output by executing <code>cd /media/HSMFD</code> <code>ttysu audit /dev/ttyUSB0</code> Note: Do not unplug USB serial port adaptor from the laptop until instructed, as this causes logging to stop.		18:36





Verify DVD checksum

Step	Activity	Initial	Time (UTC)
26	<p>In the “checksum window” CA uses the “hexread” program to have the sha256 checksum of the boot-DVD read aloud by the laptop.</p> <p><code>./hexread</code></p> <p>CA will paste the checksum into the “hexread” program at the appropriate prompt.</p> <p>If the “hexread” program fails, CA will read the checksum aloud, four digits at a time.</p> <p>EW verifies that the checksum of the boot-DVD is:</p> <p>7DE4 31F9 C33D DFEF</p> <p>9089 AB56 13A3 8126</p> <p>708A 3AC1 A784 38A7</p> <p>B9C9 2A4F 52A1 F87C</p> <p>Participants may compare this with the boot-DVD checksum calculated during Key Ceremony 6, reproduced for convenience in the appendices of this document.</p> <p>CA closes the terminal window by typing</p> <p><code>exit</code></p>		18:40




Connecting offline HSM (KSK-HSM-01B-SJC)

Step	Activity	Initial	Time (UTC)
27	<p>CA connects UPS power to the HSM. Status information will appear in the “ttyaudit window” and the “Ready” LED on the will HSM blink. After its self-test the HSM will display the text “Set Online” indicating that the HSM is in the initialized state and the “Ready” LED will be off.</p>		18:41


Activate HSM

Step	Activity	Initial	Time (UTC)
28	<p>CA sets the HSM online using the "Set Online" menu item and three of the OP cards. The "Ready" LED should illuminate.</p> <p>Use OP cards 1, 4 and 7, and PIN 11223344.</p> <p>Note that the HSM will always refer to cards 1, 2 and 3, regardless of our numbering.</p>		18:44
29	<p>CA connects Ethernet cable between laptop and HSM and tests network connectivity between laptop and HSM by entering</p> <pre>ping 192.168.0.2</pre> <p>in the "command window" and looking for responses. Press Ctrl-C to stop the ping program.</p>		18:46
30	<p>CA inserts the flash drive labeled "SCRIPTS" into a free USB slot and waits for operating system to recognize the FD. When the new window for the mounted device appears, close that window.</p>		18:48
31	<p>CA copies the compressed scripts from the drive labeled "SCRIPTS" and calculates the checksum of the tar file.</p> <pre>ls /media/SCRIPTS</pre> <pre>cp -p /media/SCRIPTS/scripts-20151123.tar.gz .</pre> <pre>sha256sum scripts-20151123.tar.gz</pre>		18:50


Start generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)
32	<p>CA copies the shell scripts that will generate new keys and bundles by executing:</p> <pre>tar -xzvof scripts-20151123.tar.gz cp -p makeallhsmfiles /opt/dccom cp -p exkey /opt/dccom cp -p keybundle-generate.20141212 /opt/dccom mkdir /tmp/pch cp -p 20151123.kc_script_gen.out /tmp/pch cp -p /opt/dnssec/aep.hsmconfig /tmp/pch</pre>		18:53
33	<p>CA copies the encrypted ZSKs by executing:</p> <pre>cd /tmp/pch makeallhsmfiles</pre>		19:16
34	<p>CA starts key and signature generation by executing:</p> <pre>keybundle-generate.20141212 < 20151123.kc_script_gen.out</pre> <p>The data file contains a line for each zone for which ZSKs will be rolled or generated. The process of generating ZSKs and KSKs and creating keybundles (KSK signed DNSKEY RRsets) will take some time. KSKs and ZSKs will automatically be received by the laptop in encrypted form and deleted from HSM as each zone is completed. The keys are stored in /tmp, which is a memory based file system.</p> <p>this step is considered complete as soon as the command is issued.</p>		19:18







Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
35	CA places each OP card with pre-printed warning slip in its own new TEB and reads the TEB number aloud. The EW records each TEB number in the smart card sign out sheet in his copy of the script, reading it aloud for verification and taking the TEB tear-off strip for his records.		19:37


Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
36	CA calls each CO to retrieve their smart cards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet and the EW initials each entry.		19:38






Smart Card Sign Out Sheet


CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410764	Steve FELDMAN		11/23/15	1938	
CO4	OP 4 of 7	A28410763	Eric ALLMAN		11/23/15	1938	
CO7	OP 7 of 7	A28410762	Gaurab UPADHAYA		11/23/15	1938	

Optionally leave facility



Step	Activity	Initial	Time (UTC)
37	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.		19:40

Pack and store Keys and Keybundles


Step	Activity	Initial	Time (UTC)
38	CA waits for key generation script to complete.		20:00
39	<p>CA generates the archive destined for the signing HSMs by executing:</p> <pre>tar -cvzf /media/HSMFD/20151123.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256 2> errors</pre> <p>The redirection of stderr to the "errors" file is to capture any error messages which may result. This file should be empty, and if so, should be deleted:</p> <pre>cat errors rm errors</pre>		20:58
40	<p>CA archives all results including encrypted KSKs for future use by executing:</p> <pre>tar -cvzf /media/HSMFD/20151123.session.tar.gz . 2> errors</pre> <pre>cat errors rm errors</pre>		20:59
41	<p>CA creates a snapshot of any changes to DB files by executing:</p> <pre>cd /media/HSMFD tar -czf 20151123.KSK-HSM-01B- SJC.db.tar.gz *.db</pre>		21:00
42	<p>CA calculates checksums of all files on the HSMFD:</p> <pre>find . -type f -print0 xargs -0 -n 50 sha256sum</pre> <p>If that command fails, the following will suffice instead:</p> <pre>sha256sum *</pre> <p>Finally, to keep an eye on available space, execute:</p> <pre>df -h</pre>		21:05

43	CA deletes the files on the SCRIPTS FD and unmounts by executing: <code>rm -rf /media/SCRIPTS/*</code> <code>umount /media/SCRIPTS</code> and removes the SCRIPTS FD for reuse.		21:05
----	--	---	-------


Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
44	CA presses the RESTART button on the HSM and waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet), placing the HSM into a new TEB and sealing it.		21:08
45	CA reads out TEB number and HSM serial number and allows participants to verify them while the EW records the TEB and HSM serial numbers here: TEB# <u>A4128460</u> HSM Serial#: <u>K1011066</u>		21:09



Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
46	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from the laptop. CA then exits out of the "ttyaudit window". <code>exit</code>		21:10


Display HSM Flash Drive Contents






Step	Activity	Initial	Time (UTC)
47	CA displays contents of HSMFD by executing: <code>ls -ltr</code>		21:10

Stop Logging Terminal Output



Step	Activity	Initial	Time (UTC)
48	CA stops logging terminal output by typing "exit" in the "command window": <code>exit</code>		21:11
49	CA calculates sha256 checksum of the logfile by executing: <code>sha256sum script-20151123.log</code> CA may use the "hexread" program to read the hash of the checksum, or read it aloud. EW records the sixty-four digit hash: <u>A2C9 172F 18A4 1B15</u> <u>33B6 F281 9594 D7ED</u> <u>D376 8156 3FEA B840</u> <u>8E86 5817 A2FB 37CA</u>		21:14

Backup HSM Flash Drive Contents



Step	Activity	Initial	Time (UTC)
50	CA plugs a blank FD labeled "HSMFD" into the laptop waits for it to be recognized by the operating system as HSMFD_ and copies the contents of the HSMFD to the blank drive by executing: <code>cp -Rp * /media/HSMFD_</code> CA then unmounts new FD using <code>umount /media/HSMFD_</code> CA then removes HSMFD_ from the laptop and places it a new TEB and seals; reads out TEB number and shows item to participants while the EW records the TEB number here: TEB# <u>A28410738</u> This copy will later be stored in the on-site audit bundle.		21:19

51	CA performs this activity a second time to create a second copy. TEB# <u>A28410739</u> This copy will later be stored in the off-site audit bundle.		21:22
52	CA performs this activity a third time to create a third copy. TEB# <u>A28410740</u> This copy will later be stored in the EW audit bundle.		21:24
53	CA performs this activity a fourth time to create a fourth copy. TEB# <u>A28410754</u> This copy will later be placed in the safe.		21:25
54	CA performs this activity a fifth time to create a fifth copy. TEB# <u>A28410755</u> This copy will later be sent to the other KSK generating country.		21:28
55	CA performs this activity a sixth time to create a sixth copy. TEB# <u>A28410756</u> This copy will later be CA's copy. CA will later upload the contents to the published archive.		21:29


Return HSMFD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
56	CA unmounts HSMFD by executing: <code>cd /tmp</code> then <code>umount /media/HSMFD</code>		21:30
57	CA removes HSMFD and places it in a new TEB and seals; reads out TEB number and shows item to participants. EW records TEB # here. TEB# <u>A 28410757</u>		21:35




Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
58	CA executes: <code>shutdown -h now</code> removes DVD and turns off laptop.		21:37
59	CA places boot-DVD in new TEB and seals; reads out TEB number and shows item to participants. EW records TEB number here: TEB# <u>A 28410758</u>		21:39


Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
60	CA disconnects power and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB number and shows item to participants. EW records TEB number here: TEB# <u>A 4128461</u>		21:42

Return Power Supplies, USB Hub, and Cables

Step	Activity	Initial	Time (UTC)
61	CA places HSM power supply and laptop power supply, USB hub, serial cable, USB serial adapter, power and networking cables in a bag. This need not be a TEB as it is only used for convenience.		21:45
62	SC returns items to the safe. SC records return of each item on the safe's log with TEB number, name of item, date, time, and signature with a second participant initialing each entry. - KSK-HSM-01B-SJC HSM - laptop - original HSMFD above - fourth HSMFD backup - DVD Power supplies and cables need not be stored in the safe if space is constrained.		21:49
63	SC records a closing action as an entry in the safe's log sheet and returns the log sheet to the safe. SC closes safe. EW verifies that it is locked.		21:49



Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
64	All participants leave the Key Management Facility, and on the Participant Signature Sheet note their exit time and sign.		21:52


Stop Audio-Visual Recording

Step	Activity	Initial	Time (PST)
65	FO stops audio and video recording.		21:53


Script review

Step	Activity	Initial	Time (UTC)
66	CA reviews EWs script and signs it: CA Signature 		21:56

Sign Out of Facility

Step	Activity	Initial	Time (PST)
67	FO returns phones, computers, and any other items to participants and logs their exit times on the facility sign-in sheet. Participants return identification vests to the FO. Participants are now free to depart.		21:57

Copy and Store the Script

Step	Activity	Initial	Time (PST)
68	<p>EW makes at least three color copies of his script: one for the off-site audit bundle, one for the on-site audit bundle, one for himself, copies for other participants as requested, and delivers the original to the SC.</p> <p>The two audit bundles each contain:</p> <ul style="list-style-type: none"> - output of signer system - HSMFD - copy of EWs key ceremony script - audio-visual recording - logs from the Facility Physical Access Control - SC attestation (A.2 below) - the EW attestation (A.1 below) <p>all in a TEB labeled "Key Ceremony 11/23/2015", dated and signed by EW and CA. One bundle will be stored by the SC along with equipment. The second bundle will be kept securely offsite.</p> <p>The fifth copy of the HSMFD will be sent to the other key signing facility.</p> <p>CA retains any remaining materials (e.g. extra HSMFD) for next key ceremony preparation and analysis.</p>		1:57

Appendix A:
Key Ceremony Script Attestation
(by EW)

I hereby attest that the Key Ceremony was conducted in accordance with this script and that any exceptions which may have occurred were accurately and properly documented on the attached Script Exception Forms.

Printed Name: _____

Larry W Jordan

Signature: _____

[Handwritten Signature]

Date: _____

11/23/2015

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

CIVIL CODE § 1189

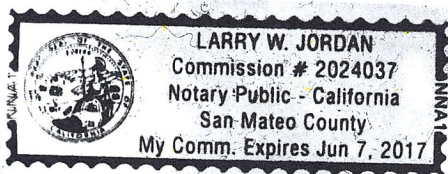
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California)
 County of San Mateo)
 On 11/23/2015 before me, Larry W. Jordan,
 Date Here Insert Name and Title of the Officer
 personally appeared William E. Woodcock
 Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.



Signature Lg W. Jordan
 Signature of Notary Public

Place Notary Seal Above

OPTIONAL

Though this section is optional, completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____ Document Date: _____
 Number of Pages: _____ Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
 Signer Is Representing: _____

Signer's Name: _____
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian or Conservator
☐ Other: _____
 Signer Is Representing: _____

Appendix B:
Access Control System Attestation
(by SC)

I have reviewed the physical access control system and not found any discrepancies or anything else out of the ordinary.

Attached is the audited physical access log.

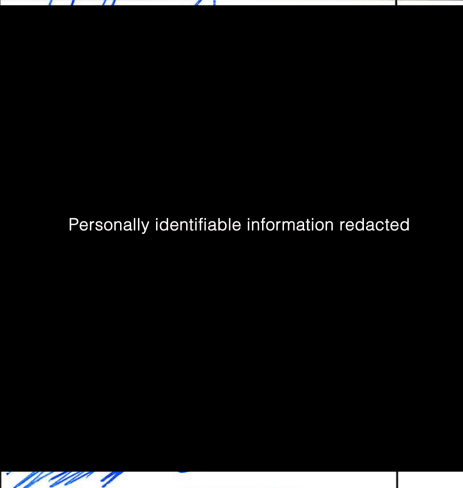
Printed Name: Bill Woodcock

Signature: 

Date: Nov 23 2015



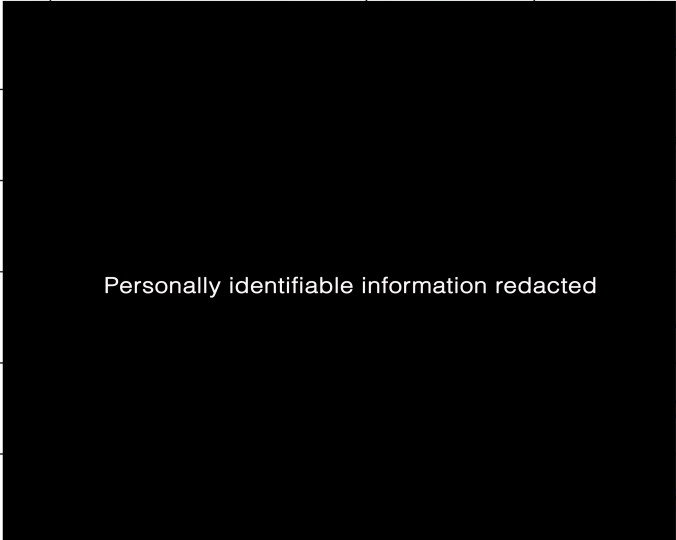
1600 Shattuck Avenue Facilities Sign-In Sheet

Role	Name	Signature	Date	Entry Time PST	Exit Time PST
FO	Peter ROWLAND	 Personally identifiable information redacted	15	9:38	14:00
CA2	Ashley JONES		15	9:32	14:00
EW	Larry JORDAN		15	9:31	14:10
CO1	Steve FELDMAN		15	9:32	13:51
CO4	Eric ALLMAN		15	9:32	13:55
CO7	Gaurab UPADHAYA		15	9:32	14:00
SC1	Bill WOODCOCK		15	9:32	13:51




PCH DNSSEC Key Ceremony Entry/Exit Log

	Name	Enter	Exit	Initial	Time
	Bruce Woodcock		X		19:40
	Ashley Jones		X		19:40
	Steve Feldman	X	X		19:40
	Gaurab Upadhyaya		X		19:41
	Eric Allman		X		19:41
	Larry Jordan		X		19:41
	Bruce Woodcock	X			20:51
	Steve Feldman	X			20:51
	Eric Allman	X			20:51
	Larry Jordan	X			20:52
	Ashley Jones	X			20:53
	Gaurab Upadhyaya	X			20:56

Participant Signature Sheet




Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
CA2	Ashley JONES		 Personally identifiable information redacted			11/23/15	17:39	21:52
EW	Larry JORDAN					11/23/15	17:38	21:52
CO1	Steve FELDMAN					11/23/15	17:41	21:51
CO4	Eric ALLMAN					11/23/15	17:41	21:52
CO7	Gaurab UPADHAYA					11/23/15	17:42	21:52
SC1	Bill WOODCOCK					11/23/15	17:40	21:51

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>EW Describes exception and action here:</p> <p>WE DISCOVERED AT STEP 33 THAT THERE WAS AN ERROR IN THE "MAKEALLHSMFILES" FILE ON THE SCRIPTS FD.</p> <p>WE DISCOVERED THAT IT CONTAINED A "FILENAME" VARIABLE WHICH WAS INCORRECTLY SET.</p> <p>WE DUPLICATED "MAKEALLHSMFILES" WITH THE NEW NAME "MAKEALLHSMFILES.20151123"</p> <p>WE SET THE "FILENAME" VARIABLE IN THE NEW COPY, AND RAN THE NEW COPY, LEAVING THE ORIGINAL COPY UNMODIFIED.</p>		19:28
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>		19:28

*** End of DNSSEC Key Ceremony Script Exception ***

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	<p>EW Describes exception and action here:</p> <p>Script Key Ceremony #14 was in error, step #12 ref. TEB # A28410722 which was HSMFD copy # 4 instead of TEB # A28410718</p>		18:01
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>		18:01

*** End of DNSSEC Key Ceremony Script Exception ***

Appendix C:

Abbreviations Used in This Document

Roles

CA	Ceremony Administrator
EW	External Witness
SC	Security Controller
CO	Crypto Officers
FO	Facilities Officer
R	Registry Representative

Other Abbreviation

TEB	Tamper Evident Bag (MMF Industries, item #2362010N20 small or #2362011N20 large)
HSM	Hardware Security Module
FD	Flash Drive
AAK	Adapter Authorization Key
SMK	Storage Master Key
OP	Operator
SO	Security Operator

Appendix D:

Letter and Number Pronunciation

Character	Call Sign	Pronunciation
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	Novemb er	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

Appendix: E

Card Distribution from Key Ceremony 1

DNSSEC Key Ceremony Script

Tuesday, April 26, 2011

Distribute Cards



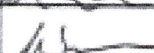







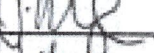

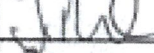
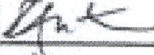
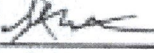




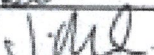

Step	Activity	Initial	Time
103	Due to limited number of personnel at this key ceremony, cards will be distributed in groups that maintain multi-person control requirements. A subsequent key ceremony will redistribute cards to their final holders. Each group of cards shall be placed in another TEB whose numbers are recorded below on the EW's script.	<i>TF</i>	8:37PM
104	SMK1, SO1, OP1 TEB# <u>A21094986</u> go to CO1, Steve FELDMAN.	<i>TF</i>	8:39PM
105	SMK5, SO5, OP5 TEB# <u>A21094983</u> are entrusted to CO1, Steve FELDMAN, for conveyance to CO6, Stephan SOMOGYI.	<i>TF</i>	8:43PM
106	SMK2, SO2, OP2 TEB# <u>A21094985</u> go to CO2, Michael SINATRA.	<i>TF</i>	8:45PM
107	SMK3, SO3, OP3 TEB# <u>A21094984</u> go to CO3, Kim DAVIES.	<i>TF</i>	8:46PM
108	SMK6, SO6, OP6 TEB# <u>A21094982</u> are entrusted to CO3, Kim DAVIES, for conveyance to CO6, LEONG Keng Thai.	<i>TF</i>	8:48PM
109	SMK4, SO4, OP4 TEB# <u>A21094980</u> go to CO4, Jonny MARTIN.	<i>TF</i>	8:49PM
110	SMK7, SO7, OP7 TEB# <u>A21094981</u> are entrusted to CO4, Jonny MARTIN, for conveyance to CO7, Gaurab UPADHAYA.	<i>TF</i>	8:50PM

Appendix: F**Smart Card Sign Out Sheet from Key Ceremony 1**

DNSSEC Key Ceremony Script

Tuesday, April 26, 2011

Smart Card Sign Out Sheet

CO#	Card Type	TES #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A21095013	Steve FELDMAN		4/25/11	10:56	1/6
CO1	SO 1 of 7	A21095012	Steve FELDMAN		4/25/11	20:56	1/6
CO1	SMK 1 of 7	A21095011	Steve FELDMAN		4/25/11	20:56	1/6
CO2	OP 2 of 7	A21095010	Michael SINATRA		4/25/11	20:55	1/6
CO2	SO 2 of 7	A21095009	Michael SINATRA		4/25/11	20:55	1/6
CO2	SMK 2 of 7	A21095008	Michael SINATRA		4/25/11	20:55	1/6
CO3	OP 3 of 7	A21095007	Kim DAVIES		4/25/11	8:52	1/6
CO3	SO 3 of 7	A21095006	Kim DAVIES		4/25/11	8:52	1/6
CO3	SMK 3 of 7	A21095004	Kim DAVIES		4/25/11	8:52	1/6
CO4	OP 4 of 7	A21095005	Jonny MARTIN		4/25/11	8:58	1/6
CO4	SO 4 of 7	A21095003	Jonny MARTIN		4/25/11	8:58	1/6
CO4	SMK 4 of 7	A21095002	Jonny MARTIN		4/25/11	8:58	1/6
CO5	OP 5 of 7	A21095001	Steve FELDMAN		4/25/11	20:50	1/6
CO5	SO 5 of 7	A21095000	Steve FELDMAN		4/25/11	20:56	1/6
CO5	SMK 5 of 7	A21094999	Steve FELDMAN		4/25/11	20:56	1/6
CO6	OP 6 of 7	A21094998	Kim DAVIES		4/25/11	8:53	1/6
CO6	SO 6 of 7	A21094997	Kim DAVIES		4/25/11	8:53	1/6
CO6	SMK 6 of 7	A21094996	Kim DAVIES		4/25/11	8:53	1/6
CO7	OP 7 of 7	A21094995	Jonny MARTIN		4/25/11	8:58	1/6
CO7	SO 7 of 7	A21094994	Jonny MARTIN		4/25/11	8:58	1/6
CO7	SMK 7 of 7	A21094993	Jonny MARTIN		4/25/11	8:58	1/6

Appendix: G**Smart Card Sign Out Sheet from Key Ceremony 2**

DNSSEC Key Ceremony Script Monday, May 30, 2011

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A19204935	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<i>[Initials]</i>
CO1	SO 1 of 7	A19204934	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<i>[Initials]</i>
CO1	SMK 1 of 7		Steve FELDMAN		5/30/11		
CO2	OP 3 of 7	A19204933	Michael SMATRA	<i>[Signature]</i>	5/30/11	0049	<i>[Initials]</i>
CO2	SO 2 of 7	A19204931	Michael SMATRA	<i>[Signature]</i>	5/30/11	0049	<i>[Initials]</i>
CO2	SMK 2 of 7		Michael SMATRA		5/30/11		
CO4	OP 4 of 7	A19204932	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<i>[Initials]</i>
CO4	SO 4 of 7	A19204930	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<i>[Initials]</i>
CO4	SMK 4 of 7		Jonny MARTIN		5/30/11		
CO5	OP 5 of 7	A19204929	Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<i>[Initials]</i>
CO5	SO 5 of 7	A19204928	Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<i>[Initials]</i>
CO5	SMK 5 of 7		Steve SOMOGYI		5/30/11		
CO7	OP 7 of 7		Jonny MARTIN		5/30/11		
CO7	SO 7 of 7		Jonny MARTIN		5/30/11		
CO7	SMK 7 of 7		Jonny MARTIN		5/30/11		

A19204944 - CO4
 A19204943 - CO1
 A19204942 - CO2
 A19204941 - CO5

Packet Clearing House Page 25 of 32

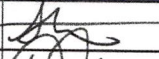

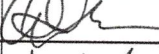

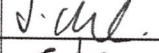





Appendix: H

Smart Card Sign Out Sheet from Key Ceremony 3

DNSSEC Key Ceremony Script

Monday, June 20, 2011

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A19204872	Steve FELDMAN		6/20/11	07:51	
CO3	OP 3 of 7	A19204874	Kim DAVIES		6/20/11	0751	
CO4	OP 4 of 7	A19204872	Jonny MARTIN		6/20/11	07:49	
CO6	OP 6 of 7	A19204870	LIM Choon Sai		6/20/11	07:50	
CO7	OP 7 of 7	A19204869	Gaurab UPADHAYA		6/20/11	07:49	

ENCLOSING BAGS:

CO1: A19204875

CO3: A19204873

CO4: A19204871

CO6: A19204869

CO7: A19204867

Appendix: I**Smart Card Sign Out Sheet from Key Ceremony 4**

DNSSEC Key Ceremony Script

Friday, January 20, 2012

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
60	CA places each OP card with instruction slip in its own new TEB and records the number in the smart card sign out sheet below.	7/	20:43

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
61	CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and EW initials their entry. Note new outer bags in sheet below.	7/	20:51

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO2	OP 2 of 7	A19204950	Michael SINATRA	Michael Sinatra	1/20/12	2051	7/
CO2	SO 2 of 7	A19204952	Michael SINATRA	Michael Sinatra	1/20/12	2051	7/
CO4	OP 4 of 7	A19204949	Jonny MARTIN	Jonny Martin	1/20/12	2049	7/
CO4	SO 4 of 7	A19204953	Jonny MARTIN	Jonny Martin	1/20/12	2049	7/
CO5	OP 5 of 7	A19204951	Stephan SOMOGYI	Stephan Somogyi	1/20/12	2046	7/
CO5	SO 5 of 7	A19204954	Stephan SOMOGYI	Stephan Somogyi	1/20/12	2046	7/

~~OUTSIDE BAG~~

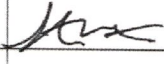



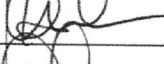

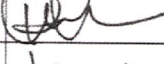

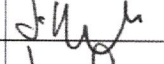

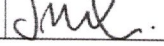

Appendix: J

Smart Card Sign Out Sheet from Key Ceremony 5


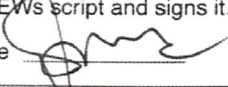

DNSSEC Key Ceremony Script

Friday, April 27, 2012


Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A19204955	Steve FELDMAN		4/27/12	18:44	
CO1	<i>Outer</i> SO 1 of 7 <i>bag</i>	3112567	Steve FELDMAN		4/27/12	18:44	
CO3	OP 3 of 7	A3112566	Kim DAVIES		4/27/12	18:46	
CO3	<i>Outer</i> SO 3 of 7 <i>Bag</i>	A3112572	Kim DAVIES		4/27/12	18:46	
CO4	OP 4 of 7	A3112565	Jonny MARTIN		4/27/12	18:47	
CO4	<i>Outer</i> SO 4 of 7 <i>bag</i>	A3112593	Jonny MARTIN		4/27/12	18:47	


Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
60	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.		18:50
61	CA reviews EW's script and signs it. CA Signature 		18:52

Sign Out of Facility

Step	Activity	Initial	Time (UTC)
62	FO returns phones, laptops, and other items to participants and logs their exit times. Participants are now free to depart.		18:53

Stop Audio-Visual Recording

Step	Activity	Initial	Time (UTC)
63	SA stops audio and video recording.		18:53

Appendix: K

Smart Card Sign Out Sheet from Key Ceremony 5-1

DNSSEC Key Ceremony Script

Wednesday, May 30, 2012

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
63	CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and EW initials their entry. Note new outer bags in sheet below.	<i>1/</i>	19:14

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410829	Steve FELDMAN	<i>[Signature]</i>	5/30/12	19:11	<i>1/</i>
CO1	<i>outer</i> SO 1 of 7	A28410826	Steve FELDMAN	<i>[Signature]</i>	5/30/12	19:11	<i>1/</i>
CO2	OP 2 of 7	A28410828	Michael SINATRA	<i>[Signature]</i>	5/30/12	19:12	<i>1/</i>
CO2	<i>outer</i> SO 2 of 7	A28410825	Michael SINATRA	<i>[Signature]</i>	5/30/12	19:12	<i>1/</i>
CO4	OP 4 of 7	A28410827	Jonny MARTIN	<i>[Signature]</i>	5/30/12	19:14	<i>1/</i>
CO4	<i>outer</i> SO 4 of 7	A28410823	Jonny MARTIN	<i>[Signature]</i>	5/30/12	19:14	<i>1/</i>

Appendix: L**Smart Card Sign Out Sheet from Key Ceremony 6**

DNSSEC Key Ceremony Script

Friday, July 27, 2012

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
67	CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and EW initials their entry. Note new outer bags in sheet below.	11	20:20

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A284/0816	Steve FELDMAN	<i>[Signature]</i>	7/27/12	2019	1
CO1	Outer 1 of 7		Steve FELDMAN		7/27/12		
CO4	OP 4 of 7	A284/0814	Jonny MARTIN	<i>[Signature]</i>	7/27/12	2019	11
CO4	Outer 4 of 7		Jonny MARTIN		7/27/12		
CO5	OP 5 of 7	A284/0817	Stephan SOMOGYI	<i>[Signature]</i>	7/27/12	2019	11
CO5	Outer 5 of 7		Stephan SOMOGYI		7/27/12		

Appendix: M**Smart Card Sign Out Sheet from Key Ceremony 7**

DNSSEC Key Ceremony Script

Friday, December 14, 2012

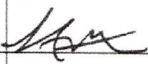
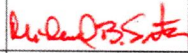

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
65	The CA places each OP card with pre-printed warning slip in its own new TEB and seals TEB, hands the EW the tear-off strip from the TEB to record.	7/	20:44

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
66	The CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and the EW initials their entry.	7/	20:46

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410805	Steve FELDMAN		12/14/12	2045	7/
CO2	OP 2 of 7	A28410804	Michael SINATRA		12/14/12	2046	7/
CO4	OP 4 of 7	A28410803	Jonny MARTIN		12/14/12	2046	7/

Appendix: N**Smart Card Sign Out Sheet from Key Ceremony 8**

Step		Activity	Initial	Time (UTC)
63	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.		JH	18:20

Re-Distribution of Cards

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410802	Steve FELDMAN		9/12/13	1912	JH
CO2	OP 2 of 7	A28410801	Michael SINATRA		9/12/13	1816	JH
CO3	OP 3 of 7	A28410800	Kim DAVIES		9/12/13	1819	JH

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
64	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.	JH	22:53
65	CA reviews EWs script and signs it. CA Signature	JH	22:55

Sign Out of Facility

Step	Activity	Initial	Time (PDT)
66	FO returns phones, laptops, and other items to participants and logs their exit times. Participants return identification vests to the FO. Participants are now free to depart.	JH	3:58 PM

Stop Audio-Visual Recording

Step	Activity	Initial	Time (PDT)
67	SA stops audio and video recording.	JH	4:00 PM

Packet Clearing House

Page 12 of 29

Appendix: O

Smart Card Sign Out Sheet from Key Ceremony 9

DNSSEC Key Ceremony Script

Friday, January 10, 2014

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
35	CA places each OP card with pre-printed warning slip in its own new TEB and records the TEB # in the EW's copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.	<i>tf</i>	18:15

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
36	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.	<i>tf</i>	18:18

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410774	Steve FELDMAN	<i>[Signature]</i>	1/10/14	18:16	<i>tf</i>
CO2	OP 2 of 7	A28410773	Michael SINATRA	<i>[Signature]</i>	1/10/14	18:17	<i>tf</i>
CO5	OP 5 of 7	A28410772	Stephan SOMOGYI	<i>[Signature]</i>	1/10/14	18:17	<i>tf</i>

Optionally leave facility

Step	Activity	Initial	Time (UTC)
37	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.	<i>tf</i>	N/A


Appendix: P

Smart Card Sign Out Sheet from Key Ceremony 10


DNSSEC Key Ceremony Script

Wednesday, March 26, 2014



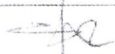



Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
35	CA places each OP card with pre-printed warning slip in its own new TEB and records the TEB # in the EW's copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.		0844

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
36	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.		0845

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO3	OP 3 of 7	Jaap AKKERHUIS	A28410778		3/26/14	0846	
CO6	OP 6 of 7	LIM Choon Sai	A28410777		3/26/14	0846	
CO7	OP 7 of 7	Gaurab UPADHAYA	A28410779		3/26/14	0846	

Optionally leave facility

Step	Activity	Initial	Time (UTC)
37	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.		

Appendix: Q**Smart Card Sign Out Sheet from Key Ceremony 11**

DNSSEC Key Ceremony Script

Friday, December 12, 2014


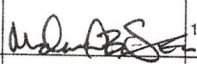

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
36	CA places each OP card with pre-printed warning slip in its own new TEB and records the TEB # in the EW's copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.	71	19:17

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
37	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.	71	19:19

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410734	Steve FELDMAN		12/12/14	19:17	71
CO2	OP 2 of 7	A28410735	Michael SINATRA		12/12/14	19:18	71
CO4	OP 4 of 7	A28410736	Eric ALLMAN		12/12/14	19:18	71

Optionally leave facility

Step	Activity	Initial	Time (UTC)
38	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.	71	

Appendix: R

Smart Card Sign Out Sheet from Key Ceremony 12

DNSSEC Key Ceremony Script

Monday, February 9, 2015

Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
35	CA places each OP card with pre-printed warning slip in its own new TEB and records the TEB # in the EW's copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.	<i>[Signature]</i>	0746

Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
36	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.	<i>[Signature]</i>	0751

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO3	OP 3 of 7	A28410768	Kim DAVIES	<i>[Signature]</i>	2/9/15	0747	<i>[Initials]</i>
CO6	OP 6 of 7	A28410767	LEE Han-Chuan	<i>[Signature]</i>	2/9/15	0747	<i>[Initials]</i>
CO7	OP 7 of 7	A28460766	Gaurab UPADHAYA	<i>[Signature]</i>	2/9/15	0748	<i>[Initials]</i>

Optionally leave facility


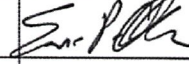

Step	Activity	Initial	Time (UTC)
37	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.	<i>[Signature]</i>	0748

Packet Clearing House

Page 10 of 37

Appendix: S

Smart Card Sign Out Sheet from Key Ceremony 13

DNSSEC Key Ceremony Script		Friday, September 25, 2015					
Re-Package OP Cards							
Step	Activity	Initial	Time (UTC)				
35	CA places each OP card with pre-printed warning slip in its own new TEB and records the TEB # in the EW's copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.	JH	19:14				
Re-Distribution of Cards							
Step	Activity	Initial	Time (UTC)				
36	CA calls each CO to retrieve their smartcards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet below and EW initials their entry.	JH	19:20				
Smart Card Sign Out Sheet							
CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410724	Steve FELDMAN		9/25/15	19:15	JH
CO4	OP 4 of 7	A28410725	Eric ALLMAN		9/25/15	19:16	JH
CO5	OP 5 of 7	A28410726	Stephan SOMOGYI		9/25/15	19:16	JH
Optionally leave facility							
Step	Activity	Initial	Time (UTC)				
37	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.	JH	19:34				
Packet Clearing House							
Page 10 of 38							

Appendix: T

Boot-DVD Checksum from Key Ceremony 6

DNSSEC Key Ceremony Script

Friday, July 27, 2012

16	CA opens a terminal window.	✓	17:18
17	<p>CA verifies the time zone, date, and time on the laptop and synchronizes it if necessary.</p> <p>Display the current time and timezone:</p> <pre>date</pre> <p>If the timezone is not set to UTC:</p> <pre>cd /etc/ rm localtime ln -s /usr/share/zoneinfo/UTC localtime</pre> <p>Set time to match the wall clock:</p> <pre>date mmddHHMMYYYY</pre> <p>Verify:</p> <pre>date</pre>	✓	17:20
18	<p>CA calculates sha256 checksum of the boot-DVD. CA may proceed with additional steps while this process completes. When the checksum is complete, CA reads it aloud, four digits at a time.</p> <pre>sha256sum /dev/cdrom</pre>	✓	17:34
19	<p>EW records the sixty-four digit boot-DVD checksum</p> <p><u>7DE4 31F9 C33D 0FFF</u> <u>9089 AB56 13A3 8126</u> <u>708A 3AC1 A784 38A7</u> <u>B9C9 2A4F 52A1 F87C</u></p> <p>Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in the appendices of this document.</p>	✓	17:34
20	CA connects USB hub to laptop.	✓	17:21
21	CA removes HSMFD KSK-HSM-01B-SJC from TEB and plugs into a free USB slot on the laptop; waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes FD window.	✓	17:29

Participants should verify the boot-DVD checksum