PCH

Packet Clearing House
572 B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
9 4 1 2 9 - 0 9 2 0   U S A
+1 415 831 3100 main
+1 415 831 3101 fax

DNSSEC Key Ceremony Script
Friday, September 25, 2015

Sign In to Facility

PDT

Step	Activity	Initial	Time (PST)
1	FO has all participants sign in on Facility Sign-In Sheet before entering the Key Management Facility.		9:49 AM
2	FO reviews emergency evacuation procedures and other relevant information with participants.		9:49 AM
3	FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility. SC is allowed to use his laptop.		9:50 AM
4	FO verifies the functioning of audio and video recording.		9:50 AM

Enter the Key Management Facility

PDt

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. Note that participants do not sign the sheet until the end of the ceremony. As the participants are identified, the identification placards are distributed.		9:51 AM

Ground Rules

PPT

Step	Activity	Initial	Time (PST)
6	CA previews ground rules and break procedures with participants. - We follow the script step by step. - Each step is read aloud by CA prior to it being performed. - When a step is complete, it is announced that it is complete plus the time. - If a participant disagree, it is important to speak up, so everyone agrees that things are done properly. - Questions and suggestions for improvement are welcome.	*(initialed)*	9:58

Verify Time and Date

PPT

Step	Activity	Initial	Time (PST)
7	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. Date: 9/25/2015 Time: 16:58 This and all subsequent entries into this script and any associated logs should follow this common source of time.	*(initialed)*	9:59

Verify UPS

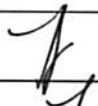| Step	Activity	Initial	Time (UTC)
8	If there is a UPS (uninterruptible power supply), then - CA makes sure the UPS is connected to the electric grid and that it is charged. - CA also makes sure that the audio recorder is plugged into the UPS.	*(initialed)*	1700

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
9	SC opens safe and makes entry in log sheet indicating opening of safe.		17:02
10	SC collects the following items from the safe: - KSK-HSM-01B-SJC HSM - boot-DVD - laptop and any other items that may be scheduled for removal indicating removal of each with corresponding TEB number in the safe log. SC also provides any necessary power supplies and cables. Equipment is placed on table visible to all partipants. If the key ceremony prior to this one was in this facility, the HSMFD is also collected from the safe. If the key ceremony prior to this one was not performed in this facility, any HSMFD from the previous key ceremony is then produced in it's TEB, having been brought in by one of the participants.		17:4p
11	CA reads out KSK-HSM-01B-SJC HSM TEB and serial number while EW checks that it matches the TEB # recorded in the script from the previous key ceremony. TEB# A3112578 Serial# K1011066		17:46
12	CA similarly reads out boot-DVD, laptop, and HSMFD TEB numbers while EW checks that they match the TEB # in the script from the previous key ceremony. DVD TEB# A28410793 Laptop TEB# A3112579 HSMFD TEB# A28410771		17:46

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 prior ceremony, 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 table, removing cards from TEBs, discarding used TEBs but saving warning slips for reuse.	*(initialed)*	17:55

Set Up Laptop

Step	Activity	Initial	Time (UTC)
14	CA takes boot-DVD and laptop out of their TEBs. CA places the boot-DVD and the laptop on the table, connects laptop power to the UPS, external monitor power can be plugged to grid power or the UPS (if the UPS is considered big enough). When these items are powered on, boot the laptop using the DVD. During the boot process, make sure the output on the laptop screen is also sent to the external monitor/projector. Booting from CD may generate warnings of kernel crash, which can be ignored if it keeps on booting.	*(initialed)*	18:04
15	CA logs in as root.	*(initialed)*	18:04
16	CA opens a terminal window.	*(initialed)*	18:05

17	CA verifies the time zone, date, and time on the laptop and synchronizes it if necessary.
	
	Display the current time and timezone:
	
	`date`
	
	If the timezone is not set to UTC:
	
	`cd /etc/`
	
	`rm localtime`
	
	`ln -s /usr/share/zoneinfo/UTC localtime`
	
	Set time to match the wall clock:
	
	`date mmddHHMMYYYY`
	
	Verify:
	
	`date`
		(signature)	18:08

18	CA disables screen saver by typing
	
	`xset s off`
	
	`(while sleep 1800;do xset -dpms;done&)`
	
	Then closes the window by typing
	
	`exit`
	
	Now, using the GUI menu, in
	
	"System" -> "Preferences" -> "Screensaver"
	
	uncheck "activate screen saver when computer is idle"
	
	Click "Close". In
	
	"System" -> "Preferences" -> "More Preferences" -> "Power Management"
	
	Ensure both sliders in "Running on AC" are set to "never".
	
	Click "Close".
		(signature)	18:10

19	CA opens a terminal window, which we will refer to as the "checksum window". In this window CA starts the calculation of the sha256 checksum of the boot-DVD. This takes about 9 minutes to complete. This step is complete after issuing this command. `sha256sum /dev/cdrom`	*(signature)*	18:10
20	CA connects USB hub to laptop.	*(signature)*	18:11

| 21 | CA removes HSMFD from the TEB, connects it to the laptop, and waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes FD window. | *(initialed)* | 18:13 |

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 new window CA will change the default directory to the HSMFD and starts capture of terminal output to a file:
	
	`cd /media/HSMFD`
	
	`script script-20150925.log`
		(initialed)	18:14

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
23	CA inspects the HSM TEB for tamper evidence and removes it from TEB; discards TEB and plugs ttyUSB0 null modem serial adaptor and cable to the back.	*(initialed)*	18:15
24	CA connects the HSM to the laptop using the USB serial adapter.	*(initialed)*	18:16

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 port output by executing
	
	`cd /media/HSMFD`
	
	`ttyaudit /dev/ttyUSB0`
	
	Note: DO not unplug USB serial port adaptor from laptop as this causes logging to stop.
		(initialed)	18:17

Verify DVD checksum

Step	Activity	Initial	Time (UTC)

26	In the "checksum window" CA uses the "hexread" program to have the sha256 checksum of the boot-DVD read aloud by the laptop.
	
	`hexread`
	
	CA will copy/paste the checksum into the "hexread" program at the appropriate prompt.
	
	If the use of the "hexread" program does not sound properly, CA will read aloud himself, four digits at a time.
	
	EW verifies that the checksum of the boot-DVD is the following:
	
	7DE4 31F9 C33D DFEF
	
	9089 AB56 13A3 8126
	
	708A 3AC1 A784 38A7
	
	B9C9 2A4F 52A1 F87C
	
	Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 6, reproduced for convenience in the appendices of this document.
	
	CA then closes the terminal window by typing
	
	`exit`
		(initialed)	18:21

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

Step	Activity	Initial	Time (UTC)
27	CA connects power to HSM. Status information will appear on the serial logging screen in the "ttyaudit window" and the "Ready" LED on the will HSM blink. After the self test the HSM display will have the text "Set Online" indicating that the HSM is in the initialized state. The "Ready" LED is off.	*(initialed)*	18:24

Activate HSM

Step	Activity	Initial	Time (UTC)
28	CA sets HSM online using the "Set Online" menu item and three (3) OP cards. The "Ready" LED should illuminate. Use OP cards 1, 4 and 5, and PIN 11223344. The HSM will always refer to cards 1, 2 and 3, regardless of our numbering (possibly) being different.		18:28
29	CA connects Ethernet cable between laptop and HSM and tests network connectivity between laptop and HSM by entering `ping 192.168.0.2` in the "command window" and looking for responses. Press Ctrl-C to stop the ping program.		18:29
30	CA inserts flash drive labeled "SCRIPTS" into a free USB slot and waits for O/S to recognize the FD. When the new window for the mounted media appears, close that window.		18:30

31	CA copies the compressed scripts from the drive labeled "SCRIPTS" and calculates the checksum of the tar-file.
	
	`ls /media/SCRIPTS`
	
	`cp -p /media/SCRIPTS/scripts-20150925.tar.gz .`
	
	`sha256sum scripts-20150925.tar.gz`
			18:31

Start generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)

32	CA copies shell scripts that will be used to generate new keys and bundles by executing:
	
	`tar -xzvof scripts-20150925.tar.gz`
	
	`cp -p makeallhsmfiles /opt/dccom`
	
	`cp -p exkey /opt/dccom`
	
	`cp -p keybundle-generate.20141212 /opt/dccom`
	
	`mkdir /tmp/pch`
	
	`cp -p 20150925.kc_script_gen.out /tmp/pch`
	
	`cp -p /opt/dnssec/aep.hsmconfig /tmp/pch`
			18:33

33	CA copies encrypted backups of the ZSKs by executing:
	
	`cd /tmp/pch`
	
	`makeallhsmfiles`
			18:33

34	CA starts key and signature generation by executing: `keybundle-generate.20141212 < 20150925.kc_script_gen.out` The data file contains a line for each zone for which ZSKs will be rolled or a new zone will be generated. This will take a long time generating ZSKs and KSKs as necessary and creating keybundles (KSK signed DNSKEY RRsets). KSKs and ZSKs will automatically be backed up in encrypted form and deleted from HSM as each zone is completed. The backed up keys are stored in /tmp, which is a memory based file system. This step is complete when the CA has issued the command above.		18:36

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.	*(initialed)*	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.	*(initialed)*	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	*(signed)*	9/25/15	1915	*(initialed)*
CO4	OP 4 of 7	A28410725	Eric ALLMAN	*(signed)*	9/25/15	19:16	*(initialed)*
CO5	OP 5 of 7	A28410726	Stephan SOMOGYI	*(signed)*	9/25/15	19:16	*(initialed)*

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.	*(initialed)*	20:34

Pack and store Keys and Keybundles

Step	Activity	Initial	Time (UTC)
38	CA waits for key generation script to complete.		20:31

39	CA generates the archive destined for the signers by executing:
	
	`tar -cvzf /media/HSMFD/20150925.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256 2> errors`
	
	The redirection of stderr to the "errors" file is to make possible error messages from the command execution easily noticable. This file should be empty:
	
	`cat errors`
	
	`rm errors`
			20:34

40	CA archives all results including encrypted KSKs for future use by executing:
	
	`tar -cvzf /media/HSMFD/20150925.session.tar.gz . 2> errors`
	
	`cat errors`
	
	`rm errors`
			20:34

41	CA creates a snapshot of any changes to DB files by executing:
	
	`cd /media/HSMFD`
	
	`tar -czf 20150925.KSK-HSM-01B-SJC.db.tar.gz *.db`
			20:35

42	CA calculates checksums of all files on the HSMFD:
	
	`find . -type f -print0 | xargs -0 -n 50 sha256sum`
	
	If that command fails, the following will suffice instead:
	
	`sha256sum *`
	
	Finally, to keep an eye on available space, execute:
	
	`df -h`
			20:36

| 43 | CA deletes the files on the SCRIPTS FD and unmounts by executing:

`rm -rf /media/SCRIPTS/*`

`umount /media/SCRIPTS`

and removes the SCRIPTS FD for reuse. | _(initialed)_ | 20:40 |

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
44	CA presses RESTART button on the HSM and waits for self test to complete. CA then disconnects HSM from power and laptop (serial and Ethernet), placing HSM into a new TEB and seals.	_(initialed)_	20:42
45	CA reads out TEB # and HSM serial #, shows item to participants while EW records TEB # and HSM serial # here. TEB# A4128457 HSM Serial#: K1011066	_(initialed)_	20:44

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". `exit`	_(initialed)_	20:44

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
47	CA displays contents of HSMFD by executing `ls -ltr`	_(initialed)_	20:45

48	CA plugs a blank FD labeled "HSMFD" into the laptop waits for it to be recognized by the O/S as HSMFD_ and copies the contents of the HSMFD to the blank drive by executing
	
	`cp -Rp * /media/HSMFD_`
	
	CA then unmounts new FD using
	
	`umount /media/HSMFD_`
	
	CA then removes HSMFD_ from the laptop and places it a new TEB and seals; reads out TEB # and shows item to participants while EW records TEB # here.
	
	TEB# A28410719
	
	This copy will later be stored in the on-site audit bundle.
			20:57

49	CA repeats this activity a second time to create a second copy. TEB# A28410720 This copy will later be stored in the off-site audit bundle.		20:59
50	CA repeats this activity a third time to create a third copy. TEB# A28410721 This copy will later be stored in the EW audit bundle.		21:01
51	CA repeats this activity a fourth time to create a fourth copy. TEB# A28410722 This copy will later be placed in the safe.		21:02
52	CA repeats this activity a fifth time to create a fifth copy. TEB# A28410723 This copy will later be sent to the other KSK generating country.		21:04

Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
53	CA stops logging terminal output by entering "exit" in "command window". `exit`		20:48
54	CA calculates sha256 checksum of the logfile by executing. `sha256sum script-20150925.log` CA may choose to use the "hexread" program, and copy/paste, to read the hash of the checksum. EW records the sixty-four digit hash 666E 17D1 EB47 68B9 2B5B 5D44 2AFF 979D A620 01CF 01DD F5ID OICF 3126 A3BC 71BA 04EE		20:53

Return HSMFD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)

55	CA unmounts HSMFD by executing
	
	`cd /tmp`
	
	then
	
	`umount /media/HSMFD`
			21:05

56	CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants. EW records TEB # here. TEB# A28410718		21:07

Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
57	CA executes: `shutdown -h now` removes DVD and turns off laptop.		21:09
58	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants. EW records TEB # here. TEB# A28410717		21:09

Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
59	CA disconnects power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants. EW records TEB # here. TEB# A4128458		21:11

Return Power Supplies, USB Hub, and Cables

Step	Activity	Initial	Time (UTC)
60	CA places HSM power supply and laptop power supply, USB hub, USB serial adapter, power and networking cables in a bag. This need not be a TEB as it is only used for convenient packaging.		21:15

61	SC returns items to the safe. SC records return of each item on the safe log with TEB #, printed name, 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 go in the safe, but can be stored separately.		21:18
62	SC closes safe. EW verifies it is locked.		21:19

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
63	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time.		2122
64	CA reviews EWs script and signs it. CA Signature		21:26

Sign Out of Facility

Step	Activity	Initial	Time (PST)
65	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.		2:26pm

Stop Audio-Visual Recording

Step	Activity	Initial	Time (PST)
66	FO stops audio and video recording.		2:26pm
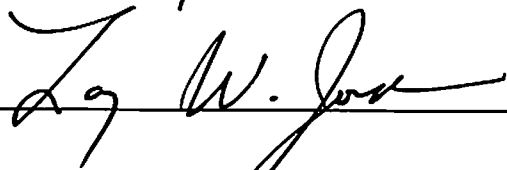
Copy and Store the Script

Step	Activity	Initial	Time (PST)
67	EW makes at least 2 colour copies of his or her script: one for off-site audit bundle, one for on-site audit bundle, copies for other participants as requested, and retaining the original. The two audit bundles each contain: - 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) all in a TEB labeled "Key Ceremony 09/25/2015", 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. The "fifth copy" of the HSMFD will be sent to the other key signing facility. CA keeps any remaining materials (e.g. extra HSMFD) for next key ceremony preparation and analysis.		

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 excpetions which may have occurred were accurately and properly documented on the attached Script Exception Forms.

Printed Name: _Larry W. Jordan_

Signature: _Larry W. Jordan_

Date: _9/25/2015_

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 _9/25/2015_ before me, _Larry W. Jordan_,
Date Here Insert Name and Title of the Officer
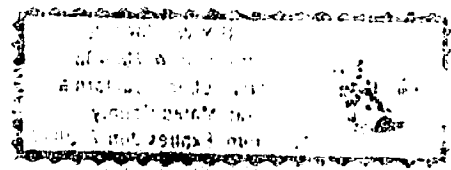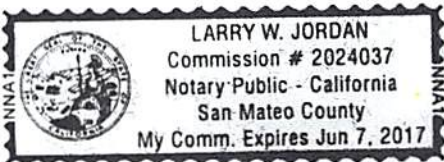
personally appeared _William E Woodcock_
Name(s) of Signer(s)

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.

> LARRY W. JORDAN
> Commission # 2024037
> Notary Public - California
> San Mateo County
> My Comm. Expires Jun 7, 2017

Signature _____
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: _Sept 25 2015_

PCH
Packet Clearing House
572 B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
9 4 1 2 9 - 0 9 2 0   U S A
+1 415 831 3100 main
+1 415 831 3101 fax

1600 Shattuck Avenue
Facilities Sign-In Sheet

PDT

Role	Name	Signature	Date	Entry Time PST	Exit Time PST
FO	Peter ROWLAND			9:45	
CA	Robert MARTIN-LEGÉNE			9:46	
EW	Larry JORDAN			9:45	
CO1	Steve FELDMAN	Personally identifiable information redacted		9:45	
CO4	Eric ALLMAN			9:45	
CO5	Stephan SOMOGYI			9:48	
SC1	Bill WOODCOCK			9:49	
R	Ashley JONES			9.48	

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	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

Appendix: E
Card Distribution from Key Ceremony 1

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.		8:37PM
104	SMK1, SD1, OP1 TEB# A21094986 go to CO1, Steve FELDMAN.		8:39PM
105	SMK5, SO5, OP5 TEB# A21094983 are entrusted to CO1, Steve FELDMAN, for conveyance to CO6, Stephan SOMOGYI		8:43PM
106	SMK2, SO2, OP2 TEB# A21094985 go to CO2, Michael SINATRA.		8:45PM
107	SMK3, SO3, OP3 TEB# A21094984 go to CO3, Kim DAVIES.		8:46PM
108	SMK6, SO6, OP6 TEB# A21094982 are entrusted to CO3, Kim DAVIES, for conveyance to CO6, LEONG Keng Thai.		8:48PM
109	SMK 4, SO4, OP4 TEB# A21094980 go to CO4, Jonny MARTIN.		8:49PM
110	SMK7, SO7, OP7 TEB# A21094981 are entrusted to CO4, Jonny MARTIN, for conveyance to CO7, Gaurab UPADHAYA.		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	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A21095013	Steve FELDMAN		4/25/11	10.56	
CO1	SO 1 of 7	A21095012	Steve FELDMAN		4/25/11	20.56	
CO1	SMK 1 of 7	A21095011	Steve FELDMAN		4/25/11	20.56	
CO2	OP 2 of 7	A21095010	Michael SINATRA		4/25/11	20.55	
CO2	SO 2 of 7	A21095009	Michael SINATRA		4/25/11	20.55	
CO2	SMK 2 of 7	A21095008	Michael SINATRA		4/25/11	20.55	
CO3	OP 3 of 7	A21095007	Kim DAVIES		4/25/11	8.52	
CO3	SO 3 of 7	A21095006	Kim DAVIES		4/25/11	8.52	
CO3	SMK 3 of 7	A21095004	Kim DAVIES		4/25/11	8.52	
CO4	OP 4 of 7	A21095005	Jonny MARTIN		4/25/11	8.58	
CO4	SO 4 of 7	A21095003	Jonny MARTIN		4/25/11	8.58	
CO4	SMK 4 of 7	A21095002	Jonny MARTIN		4/25/11	8.58	
CO5	OP 5 of 7	A21095001	Steve FELDMAN		4/25/11	20.56	
CO5	SO 5 of 7	A21095000	Steve FELDMAN		4/25/11	20.56	
CO5	SMK 5 of 7	A21094999	Steve FELDMAN		4/25/11	20.56	
CO6	OP 6 of 7	A21094998	Kim DAVIES		4/25/11	8.53	
CO6	SO 6 of 7	A21094997	Kim DAVIES		4/25/11	8.53	
CO6	SMK 6 of 7	A21094996	Kim DAVIES		4/25/11	8.53	
CO7	OP 7 of 7	A21094995	Jonny MARTIN		4/25/11	8.58	
CO7	SO 7 of 7	A21094994	Jonny MARTIN		4/25/11	8.58	
CO7	SMK 7 of 7	A21094993	Jonny MARTIN		4/25/11	8.58	

Packet Clearing House   Page 30 of 34

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	*(signature)*	5/30/11	0047	*(mark)*
CO1	SO 1 of 7	A19204934	Steve FELDMAN	*(signature)*	5/30/11	0047	*(mark)*
CO1	SMK 1 of 7		Steve FELDMAN		5/30/11		
CO2	OP 2 of 7	A19204933	Michael SINATRA	*(signature)*	5/30/11	0049	*(mark)*
CO2	SO 2 of 7	A19204931	Michael SINATRA	*(signature)*	5/30/11	0049	*(mark)*
CO2	SMK 2 of 7		Michael SINATRA		5/30/11		
CO4	OP 4 of 7	A19204932	Jonny MARTIN	*(signature)*	5/30/11	0050	*(mark)*
CO4	SO 4 of 7	A19204930	Jonny MARTIN	*(signature)*	5/30/11	0050	*(mark)*
CO4	SMK 4 of 7		Jonny MARTIN		5/30/11		
CO5	OP 5 of 7	A19204929	Stefan SOMOGYI	*(signature)*	5/30/11	0051	*(mark)*
CO5	SO 5 of 7	A19204928	Stefan SOMOGYI	*(signature)*	5/30/11	0051	*(mark)*
CO5	SMK 5 of 7		Stefan 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		

Handwritten annotations on left margin:
A19204943
A19204942
A19204944
A19204941

Handwritten notes below table:
A19204944 — C04
A19204943 — C01
A19204942 — C02
A19204941 — C05
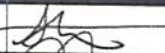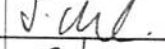
## Appendix: H

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	A 19204876	Steve FELDMAN		6/20/11	87.51	
CO3	OP 3 of 7	A 14204874	Kim DAVIES		6/20/11	0751	
CO4	OP 4 of 7	A19204872	Jonny MARTIN		6/20/11	07:49	
CO6	OP 6 of 7	A K204870	LIM Choon Sai		6/20/11	07.50	
CO7	OP 7 of 7	A19204868	Gaurab UPADHAYA		6/20/11	07.49	

ENCLOSING BAGS:

CO1: A 19204875

CO3: A 19204873

CO 4: A19204871

CO 6: A19204869

CO7: A19204867

Packet Clearing House   Page 10 of 17

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.	1/	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.	1/	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 S. Sin	1/20/12	2051	1/
CO2	SO 2 of 7	A19204952	Michael SINATRA	Michael S. Sin	1/20/12	2051	1/
CO4	OP 4 of 7	A19204949	Jonny MARTIN	JM	1/20/12	2049	1/
CO4	SO 4 of 7	A19204953	Jonny MARTIN	JM	1/20/12	2049	1/
CO5	OP 5 of 7	A19204951	Stephan SOMOGYI	S	1/20/12	2046	1/
CO5	outside bag SO 5 of 7	A19204954	Stephan SOMOGYI	SS	1/20/12	2046	1/

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	1844	
CO1	Outer SO 1 of 7 bag	3112567	Steve FELDMAN		4/27/12	1844	
CO3	OP 3 of 7	A3112566	Kim DAVIES		4/27/12	18:46	
CO3	Outer SO 3 of 7 Bag	A3112572	Kim DAVIES		4/27/12	18:46	
CO4	OP 4 of 7	A3112565	Jonny MARTIN		4/27/12	18:47	
CO4	Outer SO 4 of 7 bag	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 EWs 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

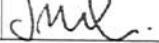Packet Clearing House   Page 11 of 24

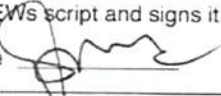## Appendix: K

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.	*[initial]*	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	*[signature]*	5/30/12	19:11	*[initial]*
CO1	outer SO 1 of 7	A28410826	Steve FELDMAN	*[signature]*	5/30/12	19:11	*[initial]*
CO2	OP 2 of 7	A28410828	Michael SINATRA	*[signature]*	5/30/12	19:12	*[initial]*
CO2	Outer SO 2 of 7	A28410825	Michael SINATRA	*[signature]*	5/30/12	19:12	*[initial]*
CO4	OP 4 of 7	A28410827	Jonny MARTIN	*[signature]*	5/30/12	19:14	*[initial]*
CO4	Outer SO 4 of 7	A28410823	Jonny MARTIN	*[signature]*	5/30/12	19:14	*[initial]*

Packet Clearing House

Page 12 of 27

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.	//	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		7/27/12	2019	/
CO1	Outer 1 of 7		Steve FELDMAN		7/27/12		
CO4	OP 4 of 7	A284/0814	Jonny MARTIN	J.M.	7/27/12	2019	//
CO4	Outer 4 of 7		Jonny MARTIN		7/27/12		
CO5	OP 5 of 7	A284/0817	Stephan SOMOGYI		7/27/12	2019	//
CO5	Outer 5 of 7		Stephan SOMOGYI		7/27/12		

Packet Clearing House
Page 12 of 28

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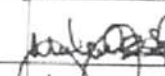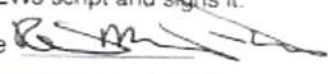
Step	Activity	Initial	Time (UTC)
66	The CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and the EW initials their entry.	7/	20:46

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A2841080 05	Steve FELDMAN		12/14/12	2045	7/
CO2	OP 2 of 7	A2841080 4	Michael SINATRA		12/14/12	2046	7/
CO4	OP 4 of 7	A2841080 3	Jonny MARTIN	J.M.Q.	12/14/12	2046	7/

Packet Clearing House   Page 13 of 30

Appendix: N

Smart Card Sign Out Sheet from Key Ceremony 8

DNSSEC Key Ceremony Script   Thursday, September 12, 2013

Re-Distribution of Cards

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		18:20

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	1712	
CO2	OP 2 of 7	A28410801	Michael SINATRA		9/12/13	816	
CO3	OP 3 of 7	A28410800	Kim DAVIES		9/12/13	1819	

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.		22:53
65	CA reviews EWs script and signs it. CA Signature		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.		3:58p

Stop Audio-Visual Recording

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

Appendix: O

Smart Card Sign Out Sheet from Key Ceremony 9
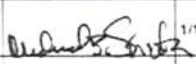
Re-Package OP Cards

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.	*ff*	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.	*ff*	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	*(signature)*	1/10/14	18:16	*ff*
CO2	OP 2 of 7	A28410773	Michael SINATRA	*(signature)*	1/10/14	18:17	*ff*
CO5	OP 5 of 7	A28410772	Stephan SOMOGYI	*(signature)*	1/10/14	18:17	*ff*

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.	*ff*	N/A

Appendix: P

Smart Card Sign Out Sheet from Key Ceremony 10

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.	*(initial)*	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.	*(initial)*	0845

Smart Card Sign Out Sheet

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

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
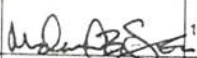
Re-Package OP Cards

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.	*(signed)*	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.	*(signed)*	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	*(signed)*	12/12/14	19:17	*(initialed)*
CO2	OP 2 of 7	A28410735	Michael SINATRA	*(signed)*	12/12/14	19:18	*(initialed)*
CO4	OP 4 of 7	A28410736	Eric ALLMAN	*(signed)*	12/12/14	19:18	*(initialed)*

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.	*(signed)*	

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 EWs copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.	_(signature)_	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 EWs copy of the sign out sheet below and EW initials their entry.	_(signature)_	0751

Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO3	OP 3 of 7	A28410768	Kim DAVIES	_(signature)_	2/9/15	0747	_(init)_
CO6	OP 6 of 7	A28410767	LEE Han-Chuan	_(signature)_	2/9/15	0747	_(init)_
CO7	OP 7 of 7	A28460766	Gaurab UPADHAYA	_(signature)_	2/9/15	0748	_(init)_

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.	_(signature)_	0748

Appendix: S

Boot-DVD Checksum from Key Ceremony 6

16	CA opens a terminal window.	𝜓	17;18

17	CA verifies the time zone, date, and time on the laptop and synchronizes it if necessary.
	
	Display the current time and timezone:
	
	`date`
	
	If the timezone is not set to UTC:
	
	`cd /etc/`
	
	`rm localtime`
	
	`ln -s /usr/share/zoneinfo/UTC localtime`
	
	Set time to match the wall clock:
	
	`date mmddHHMMYYYY`
	
	Verify:
	
	`date`
		𝜓	17:20

18	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. `sha256sum /dev/cdrom`	𝜓	17:34
19	EW records the sixty-four digit boot-DVD checksum 7DE4 3IF9 C33D 0FEF 9089 ABS6 13A3 8126 208A 3AC1 A784 38A7 B9C9 2A4F 52A1 F87C Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in the appendices of this document.	𝜓	17:34
20	CA connects USB hub to laptop.	𝜓	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.	𝜓	17:29

(handwritten margin note in red): ROTATION SCHEDULES FOR FLASH DRIVES

PCH DNSSEC Key Ceremony Entry/Exit Log   PDT

Name	Enter	Exit	Initial	Time
ROBERT MARTIN-LEGENE		X		10.09
— ,) —	X	NB		10 3 5
Eric Allman		✓	EA	12:22
Steve Feldman		✓	1328	1223
STEPHAN SOMOGYI		✓	SS	1225
BILL WOODCOCK		X	BW	12:26
ROBERT MARTIN-LEGENE		X		12:27
Larry Jordan		X		12:28
Robert Martin-Legene	X			1229
BILL WOODCOCK	X		BW	13:30
[signature]	X		LJ	13:30

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here: We going to execute 53-54 before 48-52	*(initialed)*	20:48
2	EW notes date and time of key ceremony exception and signs here: Signature: _____	*(initialed)*	20:48

* End of DNSSEC Key Ceremony Script Exception *

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here: Eric Allman and Stephan Somogyi left the ceremony without signing out	*(initials)*	2:35pm
2	EW notes date and time of key ceremony exception and signs here: Signature: *(signature)*		

* End of DNSSEC Key Ceremony Script Exception *

Participant Signature Sheet

Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
CA1	Robert MARTIN-LEGÈNE					Sept 25, 2015	16:53	2v:31
EW	Larry JORDAN					Sept 25, 2015	16:56	21:22
CO1	Steve FELDMAN					Sept 25, 2015	16:56	21:21
CO4	Eric ALLMAN					Sept 25, 2015	16:55	
CO5	Stephan SOMOGYI					Sept 25, 2015	16:54	
SC1	Bill WOODCOCK					Sept 25, 2015	16:53	21:21
R	Ashley JONES					Sept 25, 2015	16:54	19:26

Personally identifiable information redacted

PCH DNSSEC Key Ceremony Script Exception Form

Step	Activity	Initial	Time
1	EW Describes exception and action here: HSMFD TEB# A4128486 K1011066 Boot DVD TEB # A28410729 Laptop TEB # A4128487		
2	EW notes date and time of key ceremony exception and signs here: Signature:	✓	17:45

* End of DNSSEC Key Ceremony Script Exception *