

## DNSSEC Key Ceremony Script Friday, April 27, 2012

### Sign In to Facility

Step	Activity	Initial	Time (PST)
1	FO has all participants sign in before entering the Key Management Facility	<i>J</i>	9:40
2	FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility	<i>J</i>	9:40

### Emergency Evacuation Procedure

Step	Activity	Initial	Time (PST)
3	FO reviews emergency evacuation procedures and other relevant information with participants	<i>J</i>	9:00

### Enter the Key Management Facility

Step	Activity	Initial	Time (PST)
4	<p>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.</p> <p>Note that participants do not sign the sheet until the end of the ceremony.</p> <p>As the participants are identified, the EW distributes their role identification placards.</p>	<i>J</i>	16:47

Ground Rules

Step	Activity	Initial	Time (PST)
5	CA previews ground rules and break procedures with participants.	<i>TF</i>	1649

Verify Time and Date

Step	Activity	Initial	Time (UTC)
6	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: <u>4/27/12</u> Time: <u>1649</u>  This and all subsequent entries into this script and any associated logs should follow this common source of time.	<i>TF</i>	16:49

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
7	SC opens safe and makes entry in log sheet indicating opening of safe.	<i>TF</i>	1650
8	CA collects KSK-HSM-01B-SJC HSM, boot-DVD, laptop, KSK-HSM-01B-SJC HSMFD, power supplies, cables, etc. and any other items that may be scheduled for removal indicating removal of each with corresponding TEB number of safe log. Equipment is placed on table visible to all participants.	<i>TF</i>	1650
9	CA reads out KSK-HSM-01B-SJC HSM TEB and serial number while EW matches this with previous key ceremony recorded entry.  TEB# A3112557  Serial# K1011066	<i>TF</i>	1654






10	CA similarly reads out boot-DVD, laptop, and HSMFD TEB numbers while EW matches them with prior script entries.  DVD TEB# A19204948 ✓  Laptop TEB# A3112599 ✓  HSMFD KSK-HSM-01B-SJC TEB# A19204947	T/ ✓ T/ ✓	16:56 17:08
11	SC makes entry in log sheet indicating closing of safe then closes safe. EW verifies safe is locked.	T/ ✓	16:53

Collect OP Cards

Step	Activity	Initial	Time (UTC)
12	CA collects OP cards from COs, comparing TEB numbers with those recorded in the prior ceremony, reproduced for convenience in Appendix E of this document. Note any discrepancies. CA places the OP cards in plain view on the table.	T/ ✓	17:06

Set Up Laptop

Step	Activity	Initial	Time (UTC)
13	CA places the boot-DVD and laptop on the table; connects laptop power and boots laptop from DVD.	T/ ✓	17:12
14	CA logs in as root.	T/ ✓	17:13
15	CA opens a terminal window.	T/ ✓	17:14

16	<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>		17:15
17	<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>		17:15
18	<p>EW records the sixty-four digit boot-DVD checksum</p> <pre>70F4 31F9 C33D DFF F 9089 AB56 13A3 <del>8</del>26 708A 3AC1 A784 38A7 B9C9 2A4F 52A1 F87C</pre> <p>Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in Appendix F of this document.</p>		17:28
19	<p>CA connects USB hub to laptop.</p>		17:16
20	<p>CA removes HSMFD KSK-HSM-01B-SJC from TEB and plugs into a free USB slot on the laptop (NOT on expander); waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes FD window.</p>		17:18

## Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
21	CA changes the default directory to the HSMFD: <code>cd /media/HSMFD</code>	JH	17:19
22	CA starts capture of terminal output: <code>script script-20120427.log</code>	JH	17:19

## Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
23	CA connects a serial to USB null modem cable to laptop USB expander. Please note that the first USB cable connected will be "ttyUSB0", the second will be "ttyUSB1" and so on.	JH	17:20
24	CA opens a second terminal screen and ensures its default directory is also /media/HSMFD and executes <code>ttyaudit /dev/ttyUSB0</code> to start logging HSM serial port output. Note: DO NOT unplug USB serial port adaptor from laptop as this causes logging to stop.	JH	17:20

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





Step	Activity	Initial	Time (UTC)
25	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.	JH	17:21
26	CA connects power to HSM. Status information should appear on the serial logging screen and after self test the HSM display should say "Important Read Manual" indicating the HSM is in the initialized state.	JH	17:23

## Activate HSM



Step	Activity	Initial	Time (UTC)
27	CA sets HSM online ("Set Online" menu item) using three (3) OP cards. The "Ready" LED should go on.  Use 3 OP cards 1, 3 and 4.		17:25
28	CA connects Ethernet cable between laptop and HSM and tests network connectivity between laptop and HSM by entering  <code>ping 192.168.0.2</code>  on the laptop terminal window and looking for responses. Ctrl-C to exit program.		17:26

## Generate Keys and Keybundles

Step	Activity	Initial	Time (UTC)
29	CA copies shell scripts that will be used to generate new keys and bundles by plugging in SCRIPTS FD and executing:  <code>ls /media/SCRIPTS</code> <code>cp -p /media/SCRIPTS/* .</code> <code>cp -p /media/SCRIPTS/* /opt/dccom</code> <code>mkdir /tmp/pch</code> <code>cp -p *.hsm 20120427.data /tmp/pch</code>		17:32
30	CA creates encrypted backups of the ZSKs by executing  <code>cd /tmp/pch</code> then executing:  <code>keybundle-generate.20120427 &lt; 20120427.data</code>  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.	fail	18:06

31	<p>CA now archives the results onto the HSMFD by executing:</p> <pre>tar zcf /media/HSMFD/20120427.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256</pre> <p>to generate the archive destined for the signer and</p> <pre>tar zcf /media/HSMFD/20120427.session.tar.gz .</pre> <p>to archive all results including encrypted ksks for future use.</p>		18:09
32	<p>CA executes:</p> <pre>cd /media/HSMFD</pre> <pre>ls</pre> <p>to return to HSMFD and list contents.</p>		18:10
33	<p>CA creates a snapshot of any changes to DB files by executing:</p> <pre>tar zcf 20120427.KSK-HSM-01B-SJC.db.tar.gz *.db</pre>		18:10
34	<p>CA zeroizes SCRIPTS FD and unmounts by executing:</p> <pre>rm -rf /media/SCRIPTS/*</pre> <pre>umount /media/SCRIPTS</pre> <p>and removes the SCRIPTS FD for reuse.</p>		18:11

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
35	<p>CA presses RESTART button 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.</p>		18:14
36	<p>CA reads out TEB # and HSM serial #, shows item to participants while EW records TEB # and HSM serial # here.</p> <p>TEB# <u>A31/2559</u></p> <p>HSM Serial#: <u>K1011066</u></p>		18:15

Stop Recording Serial Port Activity

Step	Activity	Initial	Time (UTC)
37	CA terminates HSM serial output capture by disconnecting USB serial adaptors from laptop. CA then exits out of serial output terminal window.	<i>JH</i>	18:16

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
38	CA displays contents of HSMFD by executing <code>ls -lt</code>	<i>JH</i>	18:16
39	CA plugs a blank FD labeled "HSMFD KSK-HSM-01B-SJC" 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 for backup by executing <code>cp -Rp * /media/HSMFD_</code>	<i>JH</i>	18:17
40	CA unmounts new FD using <code>umount /media/HSMFD_</code>	<i>JH</i>	18:17
41	CA removes HSMFD_ and places it in new TEB and seals; reads out TEB # and shows item to participants while EW records TEB # here. TEB# <u>A19204958</u>	<i>JH</i>	18:19
42	CA repeats this activity a second time, to create a second backup. EW records TEB # here. TEB# _____		
43	CA repeats this activity a third time, to create a third backup. EW records TEB # here. TEB# _____		
44	CA repeats this activity a fourth time, to create a fourth backup. EW records TEB # here. TEB# _____		



## Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
45	CA stops logging terminal output by entering "exit" in remaining terminal window	<i>Jf</i>	18:19

## Return HSM FD to a Tamper Evident Bag


Step	Activity	Initial	Time (UTC)
46	CA unmounts HSMFD by executing <code>cd /tmp</code> then <code>umount /media/HSMFD</code>	<i>Jf.</i>	18:20
47	CA removes HSMFD and places it in new TEB and seals; reads out TEB # and shows item to participants.	<i>Jf</i>	18:21
48	EW records TEB # here. TEB# <u>A19204957</u>	<i>Jf</i>	18:22

## Return Boot-DVD to a Tamper Evident Bag





Step	Activity	Initial	Time (UTC)
49	After all print jobs are complete, CA executes <code>shutdown -hP now</code> removes DVD and turns off laptop.	<i>Jf</i>	18:23
50	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.	<i>Jf.</i>	18:24
51	EW records TEB # here. TEB# <u>A19204956</u>	<i>Jf</i>	18:25

## Return Laptop to a Tamper Evident Bag


Step	Activity	Initial	Time (UTC)
52	CA disconnects power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants.	<i>Jf</i>	18:26

53	EW records TEB # here. TEB# <u>A3112564</u>		18:26
----	--	---	-------


## Return Power Supplies, USB Hub, and Cables

Step	Activity	Initial	Time (UTC)
54	CA places HSM and laptop power supplies, 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.		18:28
55	SC opens safe indicating this on safe log sheet.		18:28
56	CA returns KSK-HSM-01B-SJC HSM, laptop, original HSMFD above and fourth HSMFD backup, DVD, and other items to safe. CA will record return of each item on the safe log with TEB #, printed name, date, time, and signature with a second participant initialing each entry.		18:33
57	SC closes safe. EW verifies it is locked. Two of the remaining HSMFDs will be packaged with the two audit bundles below. CA keeps any remaining materials (e.g. extra HSMFD) for next key ceremony preparation and analysis.		18:35













## Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
58	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.		18:41

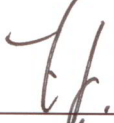
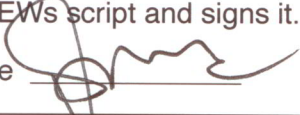

## Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
59	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.		18:48


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	<del>SO</del> 1 of 7 Outer bag	3112567	Steve FELDMAN		4/27/12	18:44	
CO3	OP 3 of 7	A3112566	Kim DAVIES		4/27/12	18:46	
CO3	<del>SO</del> 3 of 7 Outer Bag	A3112572	Kim DAVIES		4/27/12	18:46	
CO4	OP 4 of 7	A3112565	Jonny MARTIN		4/27/12	18:47	
CO4	<del>SO</del> 4 of 7 Outer 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

Copy and Store the Script

Step	Activity	Initial	Time (UTC)
64	EW makes at least 5 copies of his or her script: one for off-site audit bundle, one for on-site audit bundle, one for EW, and copies for other participants, as requested. The two audit bundles each contain 1) output of signer system - HSMFD; 2) copy of EWs key ceremony script; 3) audio-visual recording; 4) logs from the Facility Physical Access Control; 5) SA attestation (A.2 below); and 6) the EW attestation (A.1 below) - all in a TEB labeled "Key Ceremony null", 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.		

**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 Jordan

Signature: 

Date: 4/27/12

**CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT**

State of California }  
County of San Mateo }  
On 4/27/12 before me, Larry W. Jordan,  
Date Here Insert Name and Title of the Officer  
personally appeared ROBERT E. ARASMITH  
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: [Handwritten Signature]  
Signature of Notary Public

Place Notary Seal and/or Stamp Above

**OPTIONAL**

*Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another 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)**

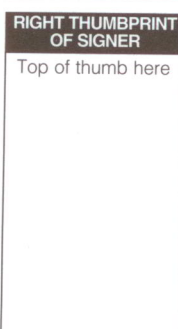
Signer's Name: \_\_\_\_\_ Signer's Name: \_\_\_\_\_

- Corporate Officer — Title(s): \_\_\_\_\_
- Individual
- Partner —  Limited  General
- Attorney in Fact
- Trustee
- Guardian or Conservator
- Other: \_\_\_\_\_



Signer Is Representing: \_\_\_\_\_

- Corporate Officer — Title(s): \_\_\_\_\_
- Individual
- Partner —  Limited  General
- Attorney in Fact
- Trustee
- Guardian or Conservator
- Other: \_\_\_\_\_



Signer Is Representing: \_\_\_\_\_

**Appendix B:**  
**Access Control System Attestation**  
**(by SA)**

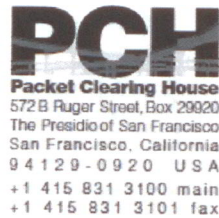
I have reviewed the physical access control system and not found any discrepancies or anything else out of the ordinary.

Attached is the audited physical access log.

Printed Name: ROBERT ARASMITA

Signature: 

Date: 4/27/12



## 1600 Shattuck Avenue Facilities Sign-In Sheet

Role	Name	Signature	Date	Entry Time PST	Exit Time PST
FO	Peter ROWLAND		4/27/12	16:40	18:50
CA1	Vicky SHRESTHA		4/27/12	16:44	18:50
EW	Larry JORDAN		4/27/12	16:45	18:56
CO1	Steve FELDMAN		4/27/12	16:44	18:50
CO3	Kim DAVIES		4/27/12	16:40	18:50
CO4	Jonny MARTIN		4/27/12	16:40	18:50
SC2	Bob ARASMITH		4/27/12	16:44	18:50
W	Bevil WOODING		4/27/12	16:41	18:50



## **Appendix C:**

### **Abbreviations Used in This Document**

#### **Roles**

CA	Ceremony Administrator
EW	External Witness
SA	System Administrator
CO	Crypto Officer
FO	Facilities Officer
W	Witness

#### **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
<b>A</b>	Alfa	AL-FAH
<b>B</b>	Bravo	BRAH-VOH
<b>C</b>	Charlie	CHAR-LEE
<b>D</b>	Delta	DELL-TAH
<b>E</b>	Echo	ECK-OH
<b>F</b>	Foxtrot	FOKS-TROT
<b>G</b>	Golf	GOLF
<b>H</b>	Hotel	HOH-TEL
<b>I</b>	India	IN-DEE-AH
<b>J</b>	Juliet	JEW-LEE-ETT
<b>K</b>	Kilo	KEY-LOH
<b>L</b>	Lima	LEE-MAH
<b>M</b>	Mike	MIKE
<b>N</b>	Novemb er	NO-VEM-BER
<b>O</b>	Oscar	OSS-CAH
<b>P</b>	Papa	PAH-PAH
<b>Q</b>	Quebec	KEH-BECK
<b>R</b>	Romeo	ROW-ME-OH
<b>S</b>	Sierra	SEE-AIR-RAH
<b>T</b>	Tango	TANG-GO
<b>U</b>	Uniform	YOU-NEE-FORM
<b>V</b>	Victor	VIK-TAH
<b>W</b>	Whiskey	WISS-KEY
<b>X</b>	Xray	ECKS-RAY
<b>Y</b>	Yankee	YANG-KEY
<b>Z</b>	Zulu	ZOO-LOO
<b>1</b>	One	WUN
<b>2</b>	Two	TOO
<b>3</b>	Three	TREE
<b>4</b>	Four	FOW-ER
<b>5</b>	Five	FIFE
<b>6</b>	Six	SIX
<b>7</b>	Seven	SEV-EN
<b>8</b>	Eight	AIT
<b>9</b>	Nine	NIN-ER
<b>0</b>	Zero	ZEE-RO

## Appendix: E

### Card Distribution from Key Ceremony 1

DNSSEC Key Ceremony Script		Tuesday, April 26, 2011	
<b>Distribute Cards</b>			
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>JJ</i>	8:37PM
104	SMK1, SO1, OP1 TEB# <u>A21094986</u> go to CO1, Steve FELDMAN.	<i>JJ</i>	8:39PM
105	SMK5, SO5, OP5 TEB# <u>A21094983</u> are entrusted to CO1, Steve FELDMAN, for conveyance to CO5, Stephan SOMOGYI.	<i>JJ</i>	8:43PM
106	SMK2, SO2, OP2 TEB# <u>A21094985</u> go to CO2, Michael SINATRA.	<i>JJ</i>	8:45PM
107	SMK3, SO3, OP3 TEB# <u>A21094984</u> go to CO3, Kim DAVIES.	<i>JJ</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>JJ</i>	8:48PM
109	SMK 4, SO4, OP4 TEB# <u>A21094980</u> go to CO4, Jonny MARTIN.	<i>JJ</i>	8:49PM
110	SMK7, SO7, OP7 TEB# <u>A21094981</u> are entrusted to CO4, Jonny MARTIN, for conveyance to CO7, Gaurab UPADHAYA.	<i>JJ</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	TEB #	Printed Name	Signature	Date	Time	EW	
-	CO1	OP 1 of 7	A21095013	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	7/6
-	CO1	SO 1 of 7	A21095012	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	7/6
-	CO1	SMK 1 of 7	A21095011	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	7/6
-	CO2	OP 2 of 7	A21095010	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	7/6
-	CO2	SO 2 of 7	A21095009	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	7/6
-	CO2	SMK 2 of 7	A21095008	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	7/6
-	CO3	OP 3 of 7	A21095007	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	7/6
-	CO3	SO 3 of 7	A21095006	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	7/6
-	CO3	SMK 3 of 7	A21095004	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	7/6
-	CO4	OP 4 of 7	A21095005	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	7/6
-	CO4	SO 4 of 7	A21095003	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	7/6
-	CO4	SMK 4 of 7	A21095002	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	7/6
-	CO5	OP 5 of 7	A21095001	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:50	7/6
-	CO5	SO 5 of 7	A21095000	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	7/6
-	CO5	SMK 5 of 7	A21094999	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:50	7/6
-	CO6	OP 6 of 7	A21094998	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	7/6
-	CO6	SO 6 of 7	A21094997	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	7/6
-	CO6	SMK 6 of 7	A21094996	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	7/6
-	CO7	OP 7 of 7	A21094995	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	7/6
-	CO7	SO 7 of 7	A21094994	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	7/6
-	CO7	SMK 7 of 7	A21094993	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	7/6

## 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
A19204943	CO1	OP 1 of 7	A19204935 Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<input checked="" type="checkbox"/>
	CO1	SO 1 of 7	A19204934 Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<input checked="" type="checkbox"/>
	CO1	SMK 1 of 7		Steve FELDMAN		5/30/11	
A19204942	CO2	OP 2 of 7	A19204933 Michael SIVATRA	<i>[Signature]</i>	5/30/11	0049	<input checked="" type="checkbox"/>
	CO2	SO 2 of 7	A19204931 Michael SIVATRA	<i>[Signature]</i>	5/30/11	0049	<input checked="" type="checkbox"/>
	CO2	SMK 2 of 7		Michael SIVATRA		5/30/11	
A19204944	CO4	OP 4 of 7	A19204932 Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<input checked="" type="checkbox"/>
	CO4	SO 4 of 7	A19204930 Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<input checked="" type="checkbox"/>
	CO4	SMK 4 of 7		Jonny MARTIN		5/30/11	
A19204941	CO5	OP 5 of 7	A19204929 Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<input checked="" type="checkbox"/>
	CO5	SO 5 of 7	A19204928 Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<input checked="" type="checkbox"/>
	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

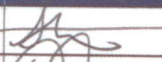
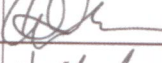
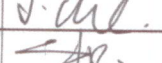

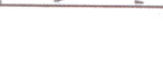
# Appendix: H

## 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	A19204876	Steve FELDMAN		6/20/11	07:51	<input checked="" type="checkbox"/>
CO3	OP 3 of 7	A19204874	Kim DAVIES		6/20/11	07:51	<input checked="" type="checkbox"/>
CO4	OP 4 of 7	A19204872	Jonny MARTIN		6/20/11	07:49	<input checked="" type="checkbox"/>
CO6	OP 6 of 7	A19204870	LIM Choon Sai		6/20/11	07:50	<input checked="" type="checkbox"/>
CO7	OP 7 of 7	A19204869	Gaurab UPADHAYA		6/20/11	07:49	<input checked="" type="checkbox"/>

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

OUTSIDE BAG

# Appendix: J

## Boot-DVD Checksum from Key Ceremony 1

DNSSEC Key Ceremony Script

Tuesday, April 26, 2011

### Set Up Laptop

Step	Activity	Initial	Time
8	CA places boot-DVD and laptop on key ceremony table; connects laptop power and boots laptop from DVD.	JJ	4:48 UTC
9	CA logs in as root.	JJ	4:49 PM
10	CA opens a terminal window.	JJ	4:49 PM
11	<p>CA verifies the timezone, date, and time on the laptop and synchronizes it if necessary.</p> <p>Display the current time and timezone: date</p> <p>If the timezone is not set to UTC: cd /etc/ rm localtime ln -s /usr/share/zoneinfo/UTC localtime</p> <p>Set time to match the wall clock: date mmddHHMMYYYY</p> <p>Verify: date</p>	JJ	4:50 PM
12	CA calculates sha256 checksum of the boot-DVD and reads it aloud, four digits at a time.	JJ	5:01 PM
13	<p>EW records the sixty-four digit boot-DVD checksum</p> <p><u>7DE4</u>   <u>31FN</u>   <u>C33D</u>   <u>DFEF</u></p> <p><u>M#08W</u>   <u>A056</u>   <u>13A3</u>   <u>8126</u></p> <p><u>708A</u>   <u>3AC1</u>   <u>A784</u>   <u>38A7</u></p> <p><u>BNC9</u>   <u>2A4F</u>   <u>52A1</u>   <u>F87C</u></p>	JJ	5:04 PM
14	CA connects USB hub to laptop.	JJ	4:55 PM
15	CA plugs blank flash disk (FD) labeled HSMFD into a free USB slot on the laptop (NOT on expander); waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes FD window.	JJ	4:55 PM

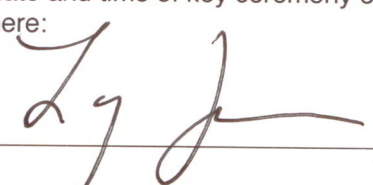


**PCH DNSSEC Key Ceremony Entry/Exit Log**

	Name	Enter	Exit	Initial	Time
1	Vicky SHRESTHA	18:03	17:46	VS	17:46
2	Steven Feldman	18:03	17:54	SMT	17:54 ft
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

**Strike out unused lines when done.**

**PCH DNSSEC Key Ceremony Script Exception Form**

Step	Activity	Initial	Time
1	<p>EW Describes exception and action here:</p> <p>HSM/FP-KSK-HSM- OIB-SJC TEB# A19204947</p> <p>Omitting Directory Directory: /media/scripts/All HSM Files</p> <p>Changes PST to UTC</p> <p>Due to script failure we are to continue <del>on</del> on Flairmate <sup>step</sup> 42, 43, 44</p> <p>1 copy for Debug not for use</p>	<p>TH</p> <p>TH</p>	<p>16:56</p> <p>17:32</p> <p>17:39</p>
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>	<p>TH</p>	<p>18:07</p>

Step 29 →

**\* 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:  Archive Everything for Debug purposes 2nd half of 31 only HFMSD <sup>Backup</sup> not <del>going</del> going into safe.	A  W	18:08  18:09
2	EW notes date and time of key ceremony exception and signs here:  Signature: _____		

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