



**Packet Clearing House**  
572 B Rucker Street, Box 29920  
The Presidio of San Francisco  
San Francisco, California  
94129-0920 USA  
+1 415 831 3100 main  
+1 415 831 3101 fax

## DNSSEC Key Ceremony Script Monday, February 9, 2015

### Sign In to Facility

Step	Activity	Initial	Time (SGT)
1	FO has all participants sign in on Facility Sign-In Sheet before entering the Key Management Facility.		1438
2	FO reviews emergency evacuation procedures and other relevant information with participants.		1438
3	FO collects cell phones, laptops, etc. Cameras are permitted in the Key Management Facility.		1438
4	FO verifies the functioning of audio and video recording.		1439.


### Enter the Key Management Facility

Step	Activity	Initial	Time (SGT)
5	<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, for them to wear.</p>		1445


Ground Rules

Step	Activity	Initial	Time (SGT)
6	CA previews ground rules and break procedures with participants.		


Verify Time and Date







Step	Activity	Initial	Time (SGT)
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: <u>9.2.2015</u> Time: <u>1448</u>  This and all subsequent entries into this script and any associated logs should follow this common source of time.		1448

Verify UPS


Step	Activity	Initial	Time (UTC)
8	CA makes sure the UPS (uninterruptible power supply) is connected to the electric grid and that it is charged.  CA also makes sure that the audio recorder is plugged into the UPS.		1449

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
9	SC opens safe and makes entry in log sheet indicating opening of safe.		0652

10	<p>SC collects the following items from the safe:</p> <ul style="list-style-type: none"> <li>- KSK-HSM-01-SIN HSM</li> <li>- boot-DVD</li> <li>- laptop</li> </ul> <p>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 participants.</p> <p>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, the HSMFD is then produced in it's TEB, having been brought in by one of the participants.</p>		<p><del>1456</del> 0656</p>	
11	<p>CA reads out KSK-HSM-01-SIN HSM TEB and serial number while EW checks that it matches the TEB # recorded in the script from the previous key ceremony.</p> <p>TEB# A3112588</p> <p>Serial# K1011055</p>		<p><del>1458</del> 0658</p>	
12	<p>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.</p> <p>DVD TEB# A28410786</p> <p>Laptop TEB# A3112589</p> <p>HSMFD TEB# A28410733</p>		<p><del>1458</del> 0658</p>	





Collect OP Cards

Step	Activity	Initial	Time (UTC)
13	<p>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.</p>		<p>0702</p>


## Set Up Laptop

Step	Activity	Initial	Time (UTC)
14	<p>CA takes boot-DVD and laptop out of their TEBs.</p> <p>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).</p> <p>When these items are powered on, boot the laptop using the DVD.</p> <p>During the boot process, make sure the output on the laptop screen is also sent to the external monitor/projector.</p> <p>Booting from CD may generate warnings of kernel crash, which can be ignored if it keeps on booting.</p>	<i>AW</i>	0708
15	CA logs in as root.	<i>AW</i>	0708
16	CA opens a terminal window.	<i>AW</i>	0709
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>	<i>AW</i>	0711






<p>18</p>	<p>CA disables screen saver by typing</p> <pre>xset s off</pre> <p>(while sleep 1800;do xset -dpms;done&amp;)</p> <p>Then closes the window by typing</p> <pre>exit</pre> <p>Now, using the GUI menu, in</p> <p>"System" -&gt; "Preferences" -&gt; "Screensaver"</p> <p>uncheck "activate screen saver when computer is idle"</p> <p>Click "Close". In</p> <p>"System" -&gt; "Preferences" -&gt; "More Preferences" -&gt; "Power Management"</p> <p>Ensure both sliders in "Running on AC" are set to "never".</p> <p>Click "Close".</p>		<p>0713</p>
<p>19</p>	<p>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.</p> <pre>sha256sum /dev/cdrom</pre>		<p>0714</p>
<p>20</p>	<p>CA connects USB hub to laptop.</p>		<p>0715</p>
<p>21</p>	<p>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.</p>		<p>0717</p>


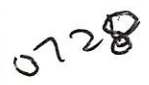
## Start Logging Terminal Session

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:  <pre>cd /media/HSMFD script script-20150209.log</pre>		0718


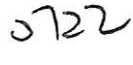
## Start Logging HSM Output

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.		0719
24	CA connects the HSM to the laptop using the USB serial adapter.		0719
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  <pre>cd /media/HSMFD ttyaudit /dev/ttyUSB0</pre> <p>Note: DO not unplug USB serial port adaptor from laptop as this causes logging to stop.</p>		0720





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> <pre>hexread</pre> <p>CA will copy/paste the checksum into the "hexread" program at the appropriate prompt.</p> <p>If the use of the "hexread" program does not sound properly, CA will read aloud himself, four digits at a time.</p> <p>EW verifies that the checksum of the boot-DVD is the following:</p> <pre>7DE4 31F9 C33D DFEF 9089 AB56 13A3 8126 708A 3AC1 A784 38A7 B9C9 2A4F 52A1 F87C</pre> <p>Other 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 then closes the terminal window by typing</p> <pre>exit</pre>		

Connecting offline HSM (KSK-HSM-01-SIN)

Step	Activity	Initial	Time (UTC)
27	<p>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.</p>		

## Activate HSM


Step	Activity	Initial	Time (UTC)
28	<p>CA sets HSM online using the "Set Online" menu item and three (3) OP cards. The "Ready" LED should illuminate.</p> <p>Use OP cards 3, 6 and 7, and PIN 11223344.</p> <p>The HSM will always refer to cards 1, 2 and 3, regardless of our numbering (possibly) being different.</p>		0724
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>		0729
30	<p>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.</p>		0730
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 cp -p /media/SCRIPTS/scripts-20150209.tar.gz . sha256sum scripts-20150209.tar.gz</pre>		0732




Start generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)
32	<p>CA copies shell scripts that will be used to generate new keys and bundles by executing:</p> <pre>tar -xzf scripts-20150209.tar.gz cp -p makeallhsmfiles /opt/dccom cp -p exkey /opt/dccom cp -p keybundle-generate.20141212 /opt/dccom mkdir /tmp/pch cp -p 20150209.kc_script_gen.out /tmp/pch cp -p /opt/dnssec/aep.hsmconfig /tmp/pch</pre>	<i>mm</i>	0735
33	<p>CA copies encrypted backups of the ZSKs by executing:</p> <pre>cd /tmp/pch makeallhsmfiles</pre>	<i>mm</i>	0736
34	<p>CA starts key and signature generation by executing:</p> <pre>keybundle-generate.20141212 &lt; 20150209.kc_script_gen.out</pre> <p>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.</p> <p>This step is complete when the CA has issued the command above.</p>	<i>mm</i>	0737





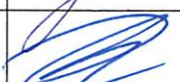

Re-Package OP Cards

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.		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.		0751






Smart Card Sign Out Sheet


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

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.		0748

## Pack and store Keys and Keybundles


Step	Activity	Initial	Time (UTC)
38	CA waits for key generation script to complete.		0752
39	CA generates the archive destined for the signers by executing:  <pre>tar -cvzf /media/HSMFD/20150209.kb.tar.gz zsk*.hsm *.keybundle.tar.gz *.keybundle.tar.gz.sha256 2&gt; errors</pre> <p>The redirection of stderr to the "errors" file is to make possible error messages from the command execution easily noticeable. This file should be empty:</p> <pre>cat errors rm errors</pre>		0754
40	CA archives all results including encrypted KSKs for future use by executing:  <pre>tar -cvzf /media/HSMFD/20150209.session.tar.gz . 2&gt; errors</pre> <pre>cat errors rm errors</pre>		0756
41	CA creates a snapshot of any changes to DB files by executing:  <pre>cd /media/HSMFD tar -czf 20150209.KSK-HSM-01-SIN.db.tar.gz *.db</pre>		0757
42	CA calculates checksums of all files on the HSMFD:  <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>		0758

43	CA deletes the files on the SCRIPTS FD and unmounts by executing:  <pre>rm -rf /media/SCRIPTS/*</pre> <pre>umount /media/SCRIPTS</pre> and removes the SCRIPTS FD for reuse.		0800
----	--	--	------


## 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.		0804
45	CA reads out TEB # and HSM serial #, shows item to participants while EW records TEB # and HSM serial # here.  TEB# <u>A 311 2585</u> HSM Serial#: <u>K1011055</u>		0805






## 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".  <pre>exit</pre>		0805



## Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
47	CA displays contents of HSMFD by executing  <pre>ls -ltr</pre>		0806





<p>48</p>	<p>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</p> <pre>cp -Rp * /media/HSMFD_</pre> <p>CA then unmounts new FD using</p> <pre>umount /media/HSMFD_</pre> <p>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.</p> <p>TEB# <u>A 28410771</u></p> <p>This copy will later be stored in the on-site audit bundle.</p>		<p>0811</p>
<p>49</p>	<p>CA repeats this activity a second time to create a second copy.</p> <p>TEB# <u>A28410770</u></p> <p>This copy will later be stored in the off-site audit bundle.</p>		<p>0813</p>
<p>50</p>	<p>CA repeats this activity a third time to create a third copy.</p> <p>TEB# <u>A28410769</u></p> <p>This copy will later be stored in the EW audit bundle.</p>		<p>0816</p>
<p>51</p>	<p>CA repeats this activity a fourth time to create a fourth copy.</p> <p>TEB# <u>A19204914</u></p> <p>This copy will later be placed in the safe.</p>		<p>0819</p>
<p>52</p>	<p>CA repeats this activity a fifth time to create a fifth copy.</p> <p>TEB# <u>A19204913</u></p> <p>This copy will later be sent to the other KSK generating country.</p>		<p>0820</p>



## Stop Logging Terminal Output

Step	Activity	Initial	Time (UTC)
53	CA stops logging terminal output by entering "exit" in "command window".  exit		0821
54	CA calculates sha256 checksum of the logfile by executing.  sha256sum script-20150209.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 <u>12A499A0 FE4E FE26</u> <u>20E173DA A2B8 8B68</u> <u>30FB362D EE42 28BC</u> <u>87136642 F21F F5FB</u>		0824


## Return HSMFD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
55	CA unmounts HSMFD by executing  cd /tmp  then  umount /media/HSMFD		0824
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# <u>A 19204912</u>		0826


## 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.		0827
58	CA places boot-DVD in new TEB and seals; reads out TEB # and shows item to participants.  EW records TEB # here. TEB# <u>A19204911</u>		0828

## Return Laptop to a Tamper Evident Bag


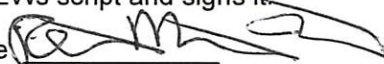

Step	Activity	Initial	Time (UTC)
59	CA disconnects power, and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB #; shows item to participants.  EW records TEB # here. TEB# <u>A3112584</u>		0830

## 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.		0831

61	<p>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.</p> <ul style="list-style-type: none"> <li>- KSK-HSM-01-SIN HSM</li> <li>- laptop</li> <li>- original HSMFD above</li> <li>- fourth HSMFD backup</li> <li>- DVD</li> </ul> <p>Power supplies and cables need not go in the safe, but can be stored separately.</p>		0835
62	SC closes safe. EW verifies it is locked.		0837


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.		0839
64	<p>CA reviews EWs script and signs it.</p> <p>CA Signature </p>		0840

Sign Out of Facility

Step	Activity	Initial	Time (SGT)
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.		0840

Stop Audio-Visual Recording

Step	Activity	Initial	Time (SGT)
66	FO stops audio and video recording.		0847




Copy and Store the Script

Step	Activity	Initial	Time (SGT)
67	<p>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.</p> <p>The two audit bundles each contain:</p> <ul style="list-style-type: none"> <li>- output of signer system - HSMFD</li> <li>- copy of EWs key ceremony script</li> <li>- audio-visual recording</li> <li>- logs from the Facility Physical Access Control</li> <li>- SC attestation (A.2 below)</li> <li>- the EW attestation (A.1 below)</li> </ul> <p>all in a TEB labeled "Key Ceremony 02/09/2015", 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 keeps any remaining materials (e.g. extra HSMFD) for next key ceremony preparation and analysis.</p>		

**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: ABDUL RAHIM SARIP

Signature: 

Date: 9/2/2015

**Insert Notary Acknowledgement Here**

**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: WILLIAM WOODCOCK

Signature:  \_\_\_\_\_

Date: FEB 8, 2015





## 1600 Shattuck Avenue Facilities Sign-In Sheet

Role	Name	Signature	Date	Entry Time SGT	Exit Time SGT
FO	GONG Wei		2/9/15		
CA	Robert MARTIN- LEGÈNE		2/9/15		
EW	Abdul Rohim SARIP		2/9/15		
CO3	Kim DAVIES		2/9/15		
CO6	LEE Han-Chuan		2/9/15		
CO7	Gaurab UPADHAYA		2/9/15		
SC1	Bill WOODCOCK		2/9/15		

## **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

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>JF</i>	8:37PM
104	SMK1, SO1, OP1 TEB# <u>A21094986</u> go to CO1, Steve FELDMAN	<i>JF</i>	8:39PM
105	SMK5, SO5, OP5 TEB# <u>A21094983</u> are entrusted to CO1, Steve FELDMAN, for conveyance to CO5, Stephen SOMOGYI	<i>JF</i>	8:43PM
106	SMK2, SO2, OP2 TEB# <u>A21094985</u> go to CO2, Michael SINATRA	<i>JF</i>	8:45PM
107	SMK3, SO3, OP3 TEB# <u>A21094984</u> go to CO3, Kim DAVIES	<i>JF</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>JF</i>	8:48PM
109	SMK4, SO4, OP4 TEB# <u>A21094980</u> go to CO4, Jonny MARTIN	<i>JF</i>	8:49PM
110	SMK7, SO7, OP7 TEB# <u>A21094981</u> are entrusted to CO4, Jonny MARTIN, for conveyance to CO7, Gaurab UPADHAYA	<i>JF</i>	8:50PM



Appendix: F

Smart Card Sign Out Sheet from Key Ceremony 1

DNSSEC Key Ceremony Script Tuesday April 28 2011

Smart Card Sign Out Sheet

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

### 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	TES #	Printed Name	Signature	Date	Time	EW
A19204943	OP 1 of 1	A19204935	Steve FELLMAN	<i>[Signature]</i>	5/30/11	0027	<input checked="" type="checkbox"/>
	SO 1 of 1	A19204934	Steve FELLMAN	<i>[Signature]</i>	5/30/11	0027	<input checked="" type="checkbox"/>
	SM 1 of 1		Steve FELLMAN		5/30/11		
A19204942	OP 2 of 1	A19204933	Michael SMATRA	<i>[Signature]</i>	5/30/11	0049	<input checked="" type="checkbox"/>
	SO 2 of 1	A19204931	Michael SMATRA	<i>[Signature]</i>	5/30/11	0049	<input checked="" type="checkbox"/>
	SM 2 of 1		Michael SMATRA		5/30/11		
A19204944	OP 4 of 1	A19204932	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<input checked="" type="checkbox"/>
	SO 4 of 1	A19204930	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<input checked="" type="checkbox"/>
	SM 4 of 1		Jonny MARTIN		5/30/11		
A19204941	OP 5 of 1	A19204929	Steve SCODGRIE	<i>[Signature]</i>	5/30/11	0051	<input checked="" type="checkbox"/>
	SO 5 of 1	A19204928	Steve SCODGRIE	<i>[Signature]</i>	5/30/11	0051	<input checked="" type="checkbox"/>
	SM 5 of 1		Steve SCODGRIE		5/30/11		
	OP 7 of 1		Jonny MARTIN		5/30/11		
	SO 7 of 1		Jonny MARTIN		5/30/11		
	SM 7 of 1		Jonny MARTIN		5/30/11		

A19204944 - C04  
 A19204943 - C01  
 A19204942 - C02  
 A19204941 - C05

Packet Clearing House Page 25 of 32

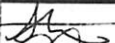





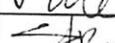



## Appendix: H

### 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	
CO3	OP 3 of 7	A19204874	Kim DAVIES		6/20/11	07:51	
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	Gaurabi 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.	T/	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.	✓	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 Sinatra</i>	1/20/12	20:51	T/
CO2	SO 2 of 7	A19204952	Michael SINATRA	<i>Michael Sinatra</i>	1/20/12	20:51	T/
CO4	OP 4 of 7	A19204949	Jonny MARTIN	<i>Jonny Martin</i>	1/20/12	20:49	T/
CO4	SO 4 of 7	A19204953	Jonny MARTIN	<i>Jonny Martin</i>	1/20/12	20:49	T/
CO6	OP 5 of 7	A19204957	Stephan SOMOGYI	<i>Stephan Somogyi</i>	1/20/12	20:46	T/
CO5	<sup>outside</sup> SO 5 of 7 <del>bag</del>	A19204954	Stephan SOMOGYI	<i>Stephan Somogyi</i>	1/20/12	20:46	T/

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	/f
CO1	<sup>Outer bag</sup> OP 2 of 7	3112567	Steve FELDMAN		4/27/12	18:44	/f
CO3	OP 3 of 7	A3112566	Kim DAVIES		4/27/12	18:46	/f
CO3	<sup>Outer bag</sup> OP 3 of 7	A3112572	Kim DAVIES		4/27/12	18:46	/f
CO4	OP 4 of 7	A3112565	Jonny MARTIN		4/27/12	18:47	/f
CO4	<sup>Outer bag</sup> OP 4 of 7	A3112593	Jonny MARTIN		4/27/12	18:47	/f

#### 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

### 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.	1/	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	1/
	Outer						
CO1	SO 1 of 7	A28410826	Steve FELDMAN	<i>[Signature]</i>	5/30/12	19:11	1/
CO2	OP 2 of 7	A28410828	Michael SINATRA	<i>[Signature]</i>	5/30/12	19:12	1/
	Outer						
CO2	SO 2 of 7	A28410825	Michael SINATRA	<i>[Signature]</i>	5/30/12	19:12	1/
CO4	OP 4 of 7	A28410827	Jonny MARTIN	<i>[Signature]</i>	5/30/12	19:14	1/
	Outer						
CO4	SO 4 of 7	A28410823	Jonny MARTIN	<i>[Signature]</i>	5/30/12	19:14	1/

## 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	A28410816	Steve FELDMAN	<i>[Signature]</i>	7/27/12	2019	11
CO1	Outer 1 of 7		Steve FELDMAN		7/27/12		
CO4	OP 4 of 7	A28410814	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	A28410817	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.	TV	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.	TV	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	<i>[Signature]</i>	12/14/12	20:45	TV
CO2	OP 2 of 7	A2840804	Michael SINATRA	<i>[Signature]</i>	12/14/12	20:46	TV
CO4	OP 4 of 7	A28410803	Jonny MARTIN	<i>[Signature]</i>	12/14/12	20:46	TV


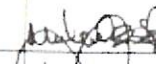



## Appendix: N

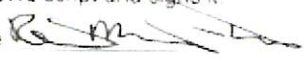
### Smart Card Sign Out Sheet from Key Ceremony 8

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	1/1	18:20

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410802	Steve FELDMAN		9/12/13	18:22	1/1
CO2	OP 2 of 7	A28410801	Michael SINATRA		9/12/13	18:16	1/1
CO3	OP 3 of 7	A28410800	Kim DAVIES		9/12/13	18:19	1/1

Step	Activity	Initial	Time (UTC)
64	All participants leave the Key Management Facility, sign the Participant Signature Sheet, and note their exit time	1/1	22:53
65	CA reviews EWs script and signs it CA Signature 	1/1	22:55

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.	1/1	3:58pm

Step	Activity	Initial	Time (PDT)
67	SA stops audio and video recording	1/1	4:00pm

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	if	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	if	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		1/10/14	18:16	if
CO2	OP 2 of 7	A28410773	Michael SINATRA		1/10/14	18:17	if
CO5	OP 5 of 7	A28410772	Stephan SOMOGYI		1/10/14	18:17	if

#### 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.	if	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	[Signature]	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	[Signature]	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	[Initials]
CO6	OP 6 of 7	Lim Choon Sui	A28410777	[Signature]	3/26/14	0846	[Initials]
CO7	OP 7 of 7	Gaurab UPADHAYA	A28410779	[Signature]	3/26/14	0846	[Initials]

**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		

Packet Clearing House Page 8 of 31

## 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.	11	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.	11	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	<i>[Signature]</i>	12/12/14	19:17	11
CO2	OP 2 of 7	A28410735	Michael SINATRA	<i>[Signature]</i>	12/12/14	19:18	11
CO4	OP 4 of 7	A28410736	Eric ALLMAN	<i>[Signature]</i>	12/12/14	19:18	11

#### 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.	11	

## Appendix: R

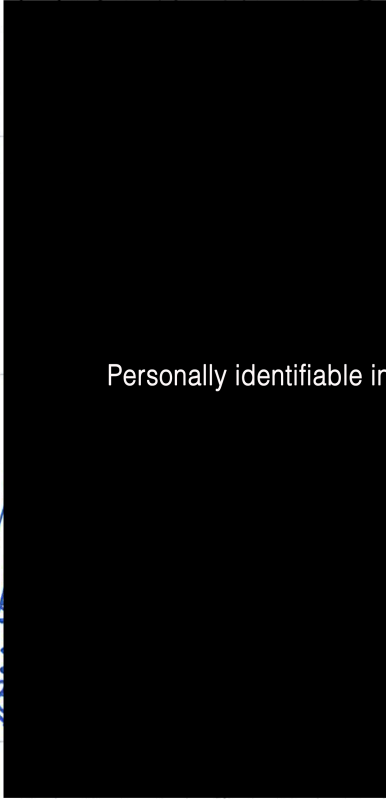
### Boot-DVD Checksum from Key Ceremony 6

DNSSEC Key Ceremony Script		Friday, July 27 2012	
16	CA opens a terminal window	<i>11</i>	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: <code>date</code>  If the timezone is not set to UTC. <code>cd /etc/</code> <code>rm localtime</code> <code>ln -s /usr/share/zoneinfo/UTC localtime</code>  Set time to match the wall clock: <code>date mmddHMMYYYY</code>  Verify <code>date</code>	<i>11</i>	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  <code>sha256sum /dev/cdrom</code>	<i>11</i>	17:34
19	EW records the sixty-four digit boot-DVD checksum <i>7DE4 31F9 C33D DFEF</i> <i>9089 ABS6 13A3 8126</i> <i>208A 3AC1 A784 38A7</i> <i>B9C9 2A4F 52A1 F87C</i>  Other participants may compare this with the boot-DVD checksum calculated during Key Ceremony 1, reproduced for convenience in the appendices of this document.	<i>11</i>	17:34
20	CA connects USB hub to laptop.	<i>11</i>	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.	<i>11</i>	17:29

*ROTATION SCHEDULES FOR FAULT-DISK*

# Participant Signature Sheet

SGT

Role	Name	Citizen ship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
CA1	Robert MARTIN-LEGÈNE		 <p>Personally identifiable information redacted</p>			February 9, 2015	1437	1648
EW	Abdul Rohim SARIP					February 9, 2015	1437	1638
CO3	Kim DAVIES					February 9, 2015	1436	1550
CO6	LEE Han-Chuan					February 9, 2015	1435	1638
CO7	Gaurab UPADHAYA					February 9, 2015	1435	1638
SC1	Bill WOODCOCK					February 9, 2015	1438	1639



### PCH DNSSEC Key Ceremony Entry/Exit Log

	Name	Enter	Exit	Initial	Time
	KIM DAVIES		0749		