



**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, February 2, 2018

### Sign In to Facility

Step	Activity	Initial	Time (PST)
1	FO has all participants sign in on Facility Sign-In Sheet before entering the Key Management Facility.	MAB	9:18 <sub>am</sub>
2	FO reviews emergency evacuation procedures and other relevant information with participants.	MAB	9:18 <sub>am</sub>
3	FO collects and stores participants' cell phones and computers outside the Key Management Facility.  Cameras and other recording devices are permitted in the Key Management Facility.  SC may retain and use a computer during the ceremony.	MAB	9:18 <sub>am</sub>
4	FO verifies the functioning of audio and video recording.	MAB	9:18 <sub>am</sub>

### Enter the Key Management Facility

Step	Activity	Initial	Time (PST)
5	As the participants enter the Key Management Facility, the EW verifies the identity of each by examining a government-issued photo identification, notes the type and number of each piece of identification, and the participant's entry time on the Participant Signature Sheet.  Participants should not sign the sheet until the end of the ceremony.  As the participants are identified each is issued an identification vest.	MAB	9:18 <sub>am</sub>

Ground Rules

Step	Activity	Initial	Time (PST)
6	<p>CA previews ground rules and break procedures with participants.</p> <ul style="list-style-type: none"> <li>- We follow the script step by step.</li> <li>- Each step is read aloud by CA prior to its performance. Text in (( double parenthesis )) does not have to be read aloud.</li> <li>- Upon the completion of each step, its completion and the time of completion are announced for the record, and the EW records the completion time and initials the EW copy of the script.</li> <li>- If any participant notices a problem or believes that an error has occurred, that participant should interrupt immediately, and the participants should agree upon a resolution prior to proceeding.</li> <li>- Any significant discrepancies or deviations from the script will be recorded by the EW on the provided Exception Sheets.</li> <li>- CA and anybody handling items removed from a TEB or items on the work surface should have rolled up sleeves or, preferably, short sleeves.</li> <li>- Ask if anybody is not known to other attendees. If not, they should be introduced.</li> <li>- Questions and suggestions for improvement are welcome at any time, will be incorporated into the record, and contribute to the quality of this and future ceremonies.</li> </ul>	<p>MAB</p>	<p>9:22am</p>

Verify Time and Date

Step	Activity	Initial	Time (PST)
7	<p>EW reads aloud and records the date (month/day/year) and time (UTC) using an NTP-synchronized clock visible to all. Participants verify that the time is correct.</p> <p>Date: <u>2.02.18</u></p> <p>Time: <u>17:20</u></p> <p>While this and previous steps are recorded using local time, subsequent steps and any associated logs follow this common source of time and are recorded in UTC.</p>	MAB	9:20am

Verify UPS

Step	Activity	Initial	Time (UTC)
8	<p>If there is a UPS (uninterruptible power supply), then</p> <ul style="list-style-type: none"> <li>- CA verifies that the UPS is connected to and receiving power from the electric grid and that it is charged.</li> <li>- CA verifies that the audio recorder is receiving power from the UPS.</li> </ul>	MAB	17:23

Remove Equipment from Safe

Step	Activity	Initial	Time (UTC)
9	SC opens the safe and records this action as an entry in the safe's log sheet.	MAB	17:25
10	SC collects the following items from the safe: - KSK-HSM-02-BRK HSM - boot-DVD - laptop ...and any other items that may be required, indicating removal of each with any applicable TEB or serial numbers in the safe's log sheet. SC also provides any necessary power supplies and cables. Equipment is placed on the work surface visible to all participants.	MAB	17:27
11	CA reads out KSK-HSM-02-BRK HSM TEB and serial numbers while EW checks that they match those recorded in the script from the most recent key ceremony performed at this site.  HSM TEB# BB69600258  HSM serial# H1411035	MAB	17:28
12	CA reads out boot-DVD and laptop TEB numbers while EW checks that they match those recorded in the script from the most recent key ceremony performed at this site.  DVD TEB# BB71705225  Laptop TEB# BB69600257	MAB	17:31

## Collect OP Cards

Step	Activity	Initial	Time (UTC)
13	<p>CA collects card wallet from CO1, inspects outer TEB, reads out and compares TEB number with that recorded in the last ceremony. CA retrieves OP1 from the card wallet, reads out and compares TEB number with that recorded in the last ceremony, then opens the TEB, placing the card in plain view on the work surface.</p> <p>(( Smart Card Sign Out Sheets from previous ceremonies are reproduced for convenience in the appendices of this document. Different COs may appear on different pages. ))</p> <p>CA collects OP cards, SO cards and SMK cards from CO4 and CO7, reading out and comparing TEB numbers with those recorded in the most recent ceremony each participated in. CA places the cards in plain view on the work surface, removing cards from TEBs.</p>	MAB	17:40

## Set Up Laptop

Step	Activity	Initial	Time (UTC)
14	<p>CA removes the boot-DVD and laptop from their TEBs, showing participants that the laptop contains no boot devices.</p> <p>CA places the boot-DVD and the laptop on the work surface, connects laptop power to the UPS. Any external monitor or projector may be powered from either the grid (or the UPS if it has sufficient capacity).</p> <p>Power the laptop on, booting it from the DVD or another boot medium.</p> <p>CA makes sure the output on the laptop screen is visible on any external monitor or projector.</p> <p>(( Use the function + F8 keys to cycle through until the display shows only on the external monitor or projector. This must be done before Linux gets past the boot loader, or you may have to reboot again until you succeed. Boot warnings may be ignored if it continues to boot. ))</p>	MAB	17:48
15	CA logs in as root.	MAB	17:49
16	CA opens a terminal window via the Menu: "Applications", "Accessories", "Terminal"	MAB	17:50

<p>17</p>	<p>CA sets the timezone on the laptop 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> <p>Repeat as needed. When pleased, close the window:</p> <pre>exit</pre>	<p>MAB</p>	<p>17:51</p>
<p>18</p>	<p>CA connects a labeled, blank HSMFD to the laptop, and waits for operating system to recognize the FD, then closes FD window.</p>	<p>MAB</p>	<p>17:52</p>

Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
19	<p>CA opens a new terminal window, which we will refer to as the "command window". In this window the CA will change the default directory to the HSMFD and start capture of terminal output to a file:</p> <pre>cd /media/HSMFD  script -t script-20180202.log 2&gt;script-20180202.timing</pre> <p>CA inserts the flash drive labeled "SCRIPTS" into a free USB slot and waits for operating system to recognize the FD. When the new window for the mounted device appears, close that window.</p> <p>CA copies the compressed archive of the previous key ceremony from the drive labeled "SCRIPTS" into the current directory on the HSMFD.</p> <pre>ls /media/SCRIPTS  cp -p /media/SCRIPTS/HSMFD-20170928.tar.gz .  sha256sum HSMFD-20170928.tar.gz</pre> <p>Verify that the checksum is 0E2C D076 95F4 6695 D126 BD3E 8097 AD89 9F82 DE21 233D FCA6 44B5 42F8 9D67 B6CE</p> <p>Un-tar the archive</p> <pre>tar -xzvof HSMFD-20170928.tar.gz</pre> <p>CA copies the compressed scripts and input files from the drive labeled "SCRIPTS" into the current directory on the HSMFD.</p> <pre>cp -p /media/SCRIPTS/scripts-20180202.tar.gz .  sha256sum scripts-20180202.tar.gz  tar -xzvof scripts-20180202.tar.gz  sh copystuff</pre>	<p>MAB</p>	<p>18:00</p>

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
20	CA inspects the HSM TEB for evidence of tampering and removes the HSM from its TEB; discards the TEB and connects the ttyUSB0 null modem serial adaptor and cable. CA connects the ttyUSB0 null modem serial adaptor and cable to the laptop, completing the serial connection between laptop and HSM.	MAB	18:03
21	CA opens a new terminal window, which we will refer to as the "ttyaudit window". In this window the CA will start logging HSM serial output by executing  <pre>cd /media/HSMFD stty -F /dev/ttyUSB0 115200 ttyaudit /dev/ttyUSB0</pre> (( Do not unplug USB serial port adaptor from the laptop until instructed, as this would cause logging to stop. ))	MAB	18:04

Connecting offline HSM (KSK-HSM-02-BRK)

Step	Activity	Initial	Time (UTC)
22	CA connects UPS power to the HSM. Status information will appear in the "ttyaudit window" and the "Ready" LED on the will HSM blink. After its self-test the HSM will display the text "Set Online" indicating that the HSM is in the initialized state and the "Ready" LED will be off.	MAB	18:07

Activate HSM

Step	Activity	Initial	Time (UTC)
23	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 7  (( All cards have PIN 11223344 ))  (( The HSM will always refer to cards 1, 2 and 3, regardless of our numbering (possibly) being different. ))	MAB	18:09



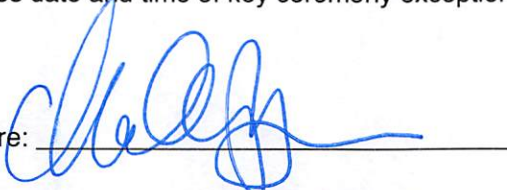
24	<p>CA connects Ethernet cable between laptop and HSM LAN port. Then determines the HSM IP in the laptop config by entering</p> <pre>ipadd</pre> <p>(( ipadd will display an internet configuration with many addresses ))</p> <pre>set-hsm-env</pre> <p>(( The script will try to ping any of the HSM's and determine which one it is talking to. It will then write the name of the connected HSM and state that it is alive. ))</p>	MAB	18:11
----	---	-----	-------

## Start generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)
25	<p>CA disables screen saver by typing</p> <pre>disable-screensaver</pre> <p>Now, using the GUI menu, in</p> <p>“System”, “Preferences”, “Screensaver”</p> <p>uncheck “activate screen saver when computer is idle”</p> <p>Click “Close”.</p> <p>In “System”, “Preferences”, “More Preferences”, “Power Management”</p> <p>Ensure both sliders in “Running on AC” are set to “never”.</p> <p>Click “Close”.</p>	MAB	18:13
26	<p>CA copies the encrypted backups of the ZSKs by executing:</p> <pre>cd /tmp/pch</pre> <pre>makeallhsmfiles</pre>	MAB	18:13

<p>27</p>	<p>CA starts key and signature generation by executing:</p> <pre>key-and-sig-gen</pre> <p>This step is considered complete as soon as the command is issued.</p> <p>(( The data file contains a line for each zone for which ZSKs will be rolled or generated. The process of generating ZSKs and KSKs and creating keybundles (KSK signed DNSKEY RRsets) will take some time. KSKs and ZSKs will automatically be received by the laptop in encrypted form and deleted from HSM as each zone is completed. The keys are stored in /tmp, which is a memory based file system. ))</p>	<p>MAB</p>	<p>18:14</p>
<p>28</p>	<p>CA may choose to open a new window and execute</p> <pre>loginspect</pre> <p>which is a tool which opens and parses the logfile.</p> <p>(( loginspect is a tool which reads from two files and tries to display a little bit of log summary while the ceremony is in progress. It may also be stopped and restarted several times, if desired, to look for events. The tool looks for elements of the key generation process which does not look like acceptable regexps. I.e. unexpected line regexps will be printed on screen. Loginspect will terminate after a period of log file inactivity, but may be started again, if it is considered that it exited prematurely. ))</p> <p>This window is only used for loginspect, and must be closed when it is considered that loginspect is no longer needed. Also, the introduction of loginspect, while tested in the lab, may fail in live key ceremonies, in which case it is not important enough to warrant a key ceremony exception.</p>	<p>MAB</p>	<p>18:10 N/A</p>

**PCH DNSSEC Key Ceremony Script Exception**

Step	Activity	Initial	Time
1	<p>During step 29, the CA noticed error messages on the screen. We completed bagging the cards in step 29, then halted the ceremony part way through step 29, and investigated the error.</p> <p>We found that the error stemmed from line 52 in the file km_one_dn_zsk_roll containing a <i>fi</i> rather than an <i>esac</i>, an improperly terminated case statement.</p> <p>We decided to correct the error and restart the ceremony from step 15bis, in order to ensure a known clean state.</p> <p>The CA edited the km_one_dn_zsk_roll file to correct the cause of the error.</p> <p>We disconnected the USB and ethernet from the HSM, but left the HSM in a powered and online state.</p> <p>We copied four files: the ttyaudit log file, the log file for the command window, the second log file for the command window containing the timing of each character sent, and the corrected version of the file "km_one_dn_zsk_roll" to SCRIPTS FD, and tarred them into file "20180202.exception.tar.gz with sha256 checksum 1B2E B376 4C07 5186 9B95 C5A2 1C31 66D0 EA47 5A7B B8F1 6AB7 4DAF E9A9 1E57 FAB8 and unmounted and disconnected the SCRIPTS FD.</p> <p>We removed all files from the HSMFD, and unmounted and disconnected the HSMFD.</p> <p>We powered the laptop off. We powered the laptop on again at 19:06, and restarted the ceremony from Step 15bis.</p> <p>As a new step 19.5bis, we copied the tarfile into the HSMFD, checksummed it for the log, extracted the corrected km_one_dn_zsk_roll file, verified that it contained the correction and was executable, and copied it to /media/HSMFD/bin and /opt/dccom, overwriting the erroneous version. Complete at 19:44.</p> <p>We skipped inapplicable portions of step 20bis and steps 22bis, 23bis and 28bis in their entirety.</p> <p>We rejoined the original script at step 29, with already bagged cards being placed into card cases.</p>	<p>MAG</p>	<p>20:07</p>
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>	<p>MAG</p>	<p>20:07</p>

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

Collect OP Cards

Step	Activity	Initial	Time (UTC)
13	<p>CA collects card wallet from CO1, inspects outer TEB, reads out and compares TEB number with that recorded in the last ceremony. CA retrieves OP1 from the card wallet, reads out and compares TEB number with that recorded in the last ceremony, then opens the TEB, placing the card in plain view on the work surface.</p> <p>(( Smart Card Sign Out Sheets from previous ceremonies are reproduced for convenience in the appendices of this document. Different COs may appear on different pages. ))</p> <p>CA collects OP cards, SO cards and SMK cards from CO4 and CO7, reading out and comparing TEB numbers with those recorded in the most recent ceremony each participated in. CA places the cards in plain view on the work surface, removing cards from TEBs.</p>	<p><i>MAB</i></p>	<p><i>19:10</i></p> <p><i>MAB</i></p>

Set Up Laptop

Step	Activity	Initial	Time (UTC)
14	<p>CA removes the boot-DVD and laptop from their TEBs, showing participants that the laptop contains no boot devices.</p> <p>CA places the boot-DVD and the laptop on the work surface, connects laptop power to the UPS. Any external monitor or projector may be powered from either the grid (or the UPS if it has sufficient capacity).</p> <p>Power the laptop on, booting it from the DVD or another boot medium.</p> <p>CA makes sure the output on the laptop screen is visible on any external monitor or projector.</p> <p>(( Use the function + F8 keys to cycle through until the display shows only on the external monitor or projector. This must be done before Linux gets past the boot loader, or you may have to reboot again until you succeed. Boot warnings may be ignored if it continues to boot. ))</p>	<p><i>MAB</i></p>	<p><i>19:18</i></p> <p><i>MAB</i></p>
15 <i>Bis</i>	CA logs in as root.	<i>MAB</i>	<i>19:20</i>
16 <i>Bis</i>	CA opens a terminal window via the Menu: "Applications", "Accessories", "Terminal"	<i>MAB</i>	<i>19:25</i>

<p>17 Bis</p>	<p>CA sets the timezone on the laptop 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> <p>Repeat as needed. When pleased, close the window:</p> <pre>exit</pre>	<p>MAB</p>	<p>19:27</p>
<p>18 Bis</p>	<p>CA connects a labeled, blank HSMFD to the laptop, and waits for operating system to recognize the FD, then closes FD window.</p>	<p>MAB</p>	<p>19:28</p>

## Start Logging Terminal Session

Step	Activity	Initial	Time (UTC)
19 BJS	<p>CA opens a new terminal window, which we will refer to as the "command window". In this window the CA will change the default directory to the HSMFD and start capture of terminal output to a file:</p> <pre>cd /media/HSMFD  script -t script-20180202.log 2&gt;script-20180202.timing</pre> <p>CA inserts the flash drive labeled "SCRIPTS" into a free USB slot and waits for operating system to recognize the FD. When the new window for the mounted device appears, close that window.</p> <p>CA copies the compressed archive of the previous key ceremony from the drive labeled "SCRIPTS" into the current directory on the HSMFD.</p> <pre>ls /media/SCRIPTS  cp -p /media/SCRIPTS/HSMFD-20170928.tar.gz .  sha256sum HSMFD-20170928.tar.gz</pre> <p>Verify that the checksum is 0E2C D076 95F4 6695 D126 BD3E 8097 AD89 9F82 DE21 233D FCA6 44B5 42F8 9D67 B6CE</p> <p>Un-tar the archive</p> <pre>tar -xzvof HSMFD-20170928.tar.gz</pre> <p>CA copies the compressed scripts and input files from the drive labeled "SCRIPTS" into the current directory on the HSMFD.</p> <pre>cp -p /media/SCRIPTS/scripts-20180202.tar.gz .  sha256sum scripts-20180202.tar.gz  tar -xzvof scripts-20180202.tar.gz  sh copystuff</pre>	MAB	19:36

Start Logging HSM Output

Step	Activity	Initial	Time (UTC)
20 BS	CA inspects the HSM TEB for evidence of tampering and removes the HSM from its TEB; discards the TEB and connects the ttyUSB0 null modem serial adaptor and cable. CA connects the ttyUSB0 null modem serial adaptor and cable to the laptop, completing the serial connection between laptop and HSM.	MAB	19:45
21 BS	CA opens a new terminal window, which we will refer to as the "ttyaudit window". In this window the CA will start logging HSM serial output by executing  <pre>cd /media/HSMFD stty -F /dev/ttyUSB0 115200 ttyaudit /dev/ttyUSB0</pre> (( Do not unplug USB serial port adaptor from the laptop until instructed, as this would cause logging to stop. ))	MAB	19:46

Connecting offline HSM (KSK-HSM-02-BRK)

Step	Activity	Initial	Time (UTC)
<del>22</del> MAB	CA connects UPS power to the HSM. Status information will appear in the "ttyaudit window" and the "Ready" LED on the will HSM blink. After its self-test the HSM will display the text "Set Online" indicating that the HSM is in the initialized state and the "Ready" LED will be off.		

Activate HSM

Step	Activity	Initial	Time (UTC)
<del>23</del> MAB	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 7  (( All cards have PIN 11223344 ))  (( The HSM will always refer to cards 1, 2 and 3, regardless of our numbering (possibly) being different. ))		

24 BS	<p>CA connects Ethernet cable between laptop and HSM LAN port. Then determines the HSM IP in the laptop config by entering</p> <pre>ipadd</pre> <p>(( ipadd will display an internet configuration with many addresses ))</p> <pre>set-hsm-env</pre> <p>(( The script will try to ping any of the HSM's and determine which one it is talking to. It will then write the name of the connected HSM and state that it is alive. ))</p>	MAB	19:47
----------	---	-----	-------

## Start generating Keys and Keybundles

Step	Activity	Initial	Time (UTC)
25 BS	<p>CA disables screen saver by typing</p> <pre>disable-screensaver</pre> <p>Now, using the GUI menu, in</p> <p>“System”, “Preferences”, “Screensaver”</p> <p>uncheck “activate screen saver when computer is idle”</p> <p>Click “Close”.</p> <p>In “System”, “Preferences”, “More Preferences”, “Power Management”</p> <p>Ensure both sliders in “Running on AC” are set to “never”.</p> <p>Click “Close”.</p>	MAB	19:49
26 BS	<p>CA copies the encrypted backups of the ZSKs by executing:</p> <pre>cd /tmp/pch</pre> <pre>makeallhsmfiles</pre>	MAB	19:49



<p>27</p>	<p>CA starts key and signature generation by executing:</p> <pre>key-and-sig-gen</pre> <p>This step is considered complete as soon as the command is issued.</p> <p>(( The data file contains a line for each zone for which ZSKs will be rolled or generated. The process of generating ZSKs and KSKs and creating keybundles (KSK signed DNSKEY RRsets) will take some time. KSKs and ZSKs will automatically be received by the laptop in encrypted form and deleted from HSM as each zone is completed. The keys are stored in /tmp, which is a memory based file system. ))</p>	<p>MAB</p>	<p>19:50</p>
<p>28</p>	<p>CA may choose to open a new window and execute</p> <pre>loginspect</pre> <p>which is a tool which opens and parses the logfile.</p> <p>(( loginspect is a tool which reads from two files and tries to display a little bit of log summary while the ceremony is in progress. It may also be stopped and restarted several times, if desired, to look for events. The tool looks for elements of the key generation process which does not look like acceptable regexps. I.e. unexpected line regexps will be printed on screen. Loginspect will terminate after a period of log file inactivity, but may be started again, if it is considered that it exited prematurely. ))</p> <p>This window is only used for loginspect, and must be closed when it is considered that loginspect is no longer needed. Also, the introduction of loginspect, while tested in the lab, may fail in live key ceremonies, in which case it is not important enough to warrant a key ceremony exception.</p>		





Re-Package OP Cards





Step	Activity	Initial	Time (UTC)
29	CA places each OP card, SO card and SMK card from each CO in its own new TEB and reads the TEB number aloud. All the cards from each CO are placed inside one smart card case. CA then places each case in its own TEB. The TEB number is read aloud. The EW records each TEB number in the smart card sign out sheet in the EW copy of the script, reading it aloud for verification.	MAB	20:20





Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
30	CA calls each CO to retrieve their smart card case. As each CO receives and inspects the TEB containing their case, they verify, date and sign the EW's copy of the sign out sheet and the EW initials each entry.	MAB	20:22

### Smart Card Sign Out Sheet

CO #	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO 1	OP 1 of 7	RA02070380	Steve FELDMAN		2/2/18	20:21	MB
CO 1	SO 1 of 7	RA02070107	Steve FELDMAN		2/2/18	11	MB
CO 1	SMK 1 of 7	RA02070109	Steve FELDMAN		2/2/18	11	MB
CO 1	Card Case	AE20992004	Steve FELDMAN		2/2/18	11	MB

CO 4	OP 4 of 7	RA02070157	Eric ALLMAN		2/2/18	20:21	MB
CO 4	SO 4 of 7	RA02070151	Eric ALLMAN		2/2/18	20:21	MB
CO 4	SMK 4 of 7	RA02070155	Eric ALLMAN		2/2/18	20:21	MB
CO 4	Card Case	AE20992000	Eric ALLMAN		2/2/18	20:21	MB

CO 7	OP 7 of 7	RA02070382	Gaurab UPADHAYA		2/2/18	20:22	MB
CO 7	SO 7 of 7	RA02070384	Gaurab UPADHAYA		2/2/18	20:22	MB
CO 7	SMK 7 of 7	RA02070149	Gaurab UPADHAYA		2/2/18	20:22	MB
CO 7	Card Case	AE20992008	Gaurab UPADHAYA		2/2/18	20:22	MB

Leave facility

Step	Activity	Initial	Time (UTC)
31	All participants will now leave the room, and be noted on the appropriate signout sheets.	MAS	20:31
32	<p><del>FO enters the room and</del> stops the audio recording.                      SC1                      The door is closed and sealed.</p> <p>One camera at a time, such that there is continuous video recording, FO will modify the video recordings to be timelapsed.</p>	MAS	20:34

Reenter facility

Step	Activity	Initial	Time (UTC)
33	When the key generation script is complete; one camera at a time, such that there is continuous video recording, FO will modify the video system to do realtime recording.  SA inspects the door's seal together with the CA, then SA enters the room alone and starts the audio recording, then immediately signs in, in the following step.	MAB	17:15
34	Participants will now enter the room, and be noted on the appropriate sheets.	MAB	17:18


Verify Time and Date

Step	Activity	Initial	Time (PST)
35	EW reads aloud and records the date (month/day/year) and time (UTC) using the clock visible to all. Participants verify that the time is correct.  Date: <u>2.05.18</u> Time: <u>17:19</u>  (( This step is recorded using local time, subsequent steps use UTC ))	MAB	9:19 am

Import Additional Script Changes

Step	Activity	Initial	Time (UTC)
36	CA unmounts the SCRIPTS FD by executing:  <code>umount /media/SCRIPTS</code>  and removes the SCRIPTS FD  (( The SCRIPTS FD will not need a TEB but can be reused at next KC. ))	MAB	17:19

**PCH DNSSEC Key Ceremony Script Exception Form**

Step	Activity	Initial	Time
1	<p>At Step 37, we found ourselves in /tmp/pch when the script was expecting /media/HSMFD. We cd to /media/HSMFD and resume Step 37.</p> <p>At Step 39 we needed to be back in /tmp/pch, so we cd back to /tmp/pch and resume Step 39.</p>	MAB	17:34
2	<p>EW notes date and time of key ceremony exception and signs here:</p> <p>Signature: </p>	MAB	17:34

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

37	<p>CA inserts another flash drive labeled "SCRIPTS" and waits for operating system to recognize the FD. When the new window for the mounted device appears, close that window.</p> <p>This FD contains updated scripts which have been modified to handle multi-day ceremonies.</p> <p>CA copies the compressed scripts from the drive labeled "SCRIPTS" into the current directory on the HSMFD.</p> <pre>cp -p /media/SCRIPTS/scripts-20180202extra.tar.gz .</pre> <p>CA unmounts the SCRIPTS FD by executing:</p> <pre>umount /media/SCRIPTS</pre> <p>and removes the SCRIPTS FD.</p> <p>To calculate checksum, execute:</p> <pre>sha256sum scripts-20180202extra.tar.gz</pre>	MAB	17:23
38	<p>To extract and copy the new files:</p> <pre>tar -xzvof scripts-20180202extra.tar.gz</pre> <pre>cp -p copystuff pack-hsmfd pack-snapshot-db pack-today-kb pack-today-session bin/</pre> <pre>chmod a+rx bin/*</pre> <pre>cp -p bin/* /opt/dccom</pre> <p>and finally to override each script's belief that the KC started today, by executing:</p> <pre>export kcdate=20180202</pre>	MAB	17:25

## Pack and store Keys and Keybundles

Step	Activity	Initial	Time (UTC)
39	<p>CA generates the archive destined for the signing HSMs by executing:</p> <pre>pack-today-kb</pre>	MAB	17:35
40	<p>CA archives all results including encrypted KSKs for future use by executing:</p> <pre>pack-today-session</pre>	MAB	17:35

41	CA creates a snapshot of any changes to DB files by executing:  <code>cd /media/HSMFD</code> <code>pack-snapshot-db KSK-HSM-02-BRK</code>	MAB	17:36
42	CA calculates checksums of all files on the HSMFD:  <code>find . -type f -print0   xargs -0 -n 50 sha256sum</code>  To keep an eye on available space on the HSMFD, execute:  <code>df -h</code>	MAB	17:38

Return HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
43	CA presses the RESTART button on the HSM and waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet), placing the HSM into a new TEB and sealing it.	MAB	17:42
44	CA reads out TEB number and HSM serial number and allows participants to verify them while the EW records the TEB and HSM serial numbers here:  TEB# <del>BB09600253</del> <sup>BB09600253</sup> HSM Serial#: <del>1411035</del> <sup>1411035</sup>	MAB	17:45

Stop Recording Serial Port Activity


Step	Activity	Initial	Time (UTC)
45	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from the laptop. CA then exits out of the "ttyaudit window".  <code>exit</code>	MAB	17:45

Display HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
46	CA displays contents of HSMFD by executing:  <code>ls -ltr</code>	MAB	17:45



**PCH DNSSEC Key Ceremony Script Exception Form**

Step	Activity	Initial	Time
1	At Step 49, we encountered an error resulting from the multi-day nature of the key ceremony. The written script referenced the archive file name HSMFD-20180202.tar.gz, while the machine-readable script generated HSMFD-20180205.tar.gz. We completed the step with the 20180205 date, calculating the checksum, and then renamed the file HSMFD-20180202.tar.gz so as to avoid more exceptions further into the script.	MAB	17:59
2	EW notes date and time of key ceremony exception and signs here:  Signature: 	MAB	17:59

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

Stop Logging and create archive

Step	Activity	Initial	Time (UTC)
47	CA stops logging terminal output by typing "exit" in the "command window":  <code>exit</code>	MAB	17:46
48	Pack it all up into a single archive:  <code>pack-hsmfd</code>	MAB	17:49
49	CA calculates sha256 checksum of the archive by executing:  <code>sha256sum HSMFD-20180202.tar.gz</code>  CA reads the hash of the checksum aloud.  EW records the sixty-four digit hash:  <u>6C3A8D60 20 504D E949</u> <u>97BD 74DA CFA2 F94F</u> <u>245E E13A AFB9 6244</u> <u>C642 17A1 703E D1FA</u>	MAB	17:53

Backup HSM Flash Drive Contents

Step	Activity	Initial	Time (UTC)
50	CA plugs a blank FD labeled "HSMFD" into the laptop waits for it to be recognized by the operating system as HSMFD_ and copies the tar-archive of the HSMFD to the blank drive by executing:  <code>cp -p HSMFD-20180202.tar.gz /media/HSMFD_</code>  CA then unmounts new FD using  <code>umount /media/HSMFD_</code>  CA then removes HSMFD_ from the laptop and places it in a new TEB and seals; reads out TEB number and shows item to participants while the EW records the TEB number here:  TEB# <u>BB71705232</u>  (( This copy will later be stored in the on-site audit bundle / safe. ))	MAB	18:04

51	CA performs this activity a second time to create a second copy. TEB# <u>BB71705228</u> (( This copy will later be stored in the off-site audit bundle. ))	MAB	18:07
----	--	-----	-------

## Unmounting HSMFD

Step	Activity	Initial	Time (UTC)
52	CA unmounts HSMFD by executing: <code>cd /tmp</code> then <code>umount /media/HSMFD</code>	MAB	18:07
53	CA removes HSMFD and keeps it for himself (( for operations and published archive ))	MAB	18:08

## Return Boot-DVD to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
54	CA executes: <code>halt -p -f</code> removes DVD and turns off laptop. To remove DVD, CA may need to briefly power on laptop, press eject button, and power off. (( we don't have to shut down nicely, as we have nowhere to write, no important services to terminate nicely and no read-write mounts to unmount ))	MAB	18:09
55	CA places boot-DVD in new TEB and seals; reads out TEB number and shows item to participants. EW records TEB number here: DVD TEB# <u>BB71705227</u>	MAB	18:10

Return Laptop to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
56	<p>CA disconnects power and any other connections from laptop and puts laptop in new TEB and seals; reads out TEB number and shows item to participants.</p> <p>EW records TEB number here: Laptop TEB# <u>BB69600254</u></p>	<p>MTB</p>	<p>18:11</p>

Return Power Supplies and Cables

Step	Activity	Initial	Time (UTC)
57	<p>CA places the following in a box or bag. This need not be a TEB as it is only used for convenience.</p> <ul style="list-style-type: none"> <li>- HSM power supply</li> <li>- Laptop power supply</li> <li>- Serial cable</li> <li>- USB serial adapter</li> <li>- Networking cables</li> </ul>	<p>MTB</p>	<p>18:14</p>
58	<p>SC returns items to the safe. SC records return of each item on the safe's log with TEB number, name of item, date, time, and signature with a second participant initialing each entry.</p> <ul style="list-style-type: none"> <li>- KSK-HSM-02-BRK HSM</li> <li>- laptop</li> <li>- HSMFD 1 above</li> <li>- DVD</li> </ul> <p>Power supplies and cables need not be stored in the safe if space is constrained.</p> <p>SC records a closing action as an entry in the safe's log sheet and returns the log sheet to the safe. SC closes safe. EW verifies that it is locked.</p>	<p>MTB</p>	<p>18:19</p>

Sign-Out on Participant Signature Sheet

Step	Activity	Initial	Time (UTC)
------	----------	---------	------------

59	All participants leave the Key Management Facility, and on the Participant Signature Sheet note their exit time and sign.	MAB	18:20
----	---	-----	-------

Stop Audio-Visual Recording

Step	Activity	Initial	Time (PST)
60	FO stops audio and video recording.	MAB	18:22

Script review

Step	Activity	Initial	Time (UTC)
61	CA reviews EWs script and signs it: CA Signature 	MAB	18:25

Sign Out of Facility

Step	Activity	Initial	Time (PST)
62	FO returns phones, computers, and any other items to participants and logs their exit times on the facility sign-in sheet. Participants return identification vests to the FO. Participants are now free to depart.	MAB	10:26am

Attestations

Step	Activity	Initial	Time (PST)
63	SC completes Access Control System Attestation in Appendix A. EW completes Key Ceremony Script Attestation in Appendix B. EW completes notary attestation.	MAB	10:33am

Copy and Store the Script

Step	Activity	Initial	Time (PST)
64	<p>FO makes at least three color copies of the EW's script: one for the off-site audit bundle, one for the on-site audit bundle, one for the EW, copies for other participants as requested, and delivers the original to the SC.</p> <p>The two audit bundles each contain hard copies and soft copies on an SD card:</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 Access Control</li> <li>- SC attestation (Appendix A below)</li> <li>- the EW attestation (Appendix B below)</li> </ul> <p>all in a TEB labeled "Key Ceremony 02/02/2018", dated and signed by CA. One bundle will be stored by the SC along with equipment. The second bundle will be kept securely offsite.</p> <p>CA will upload soft copies of all of the above to pch.net.</p>		

**Appendix A:**  
**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: MON FEB 5 2018

**Appendix B:**  
**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: Mallory Barrera

Signature: 

Date: 2.5.18



**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 Alameda )

On 2.5.18 before me, Mallory Barrera, Notary Public  
Date Here Insert Name and Title of the Officer

personally appeared Bill Woodcock  
Name(s) of Signer(s)

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

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

WITNESS my hand and official seal.



Signature [Handwritten 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**

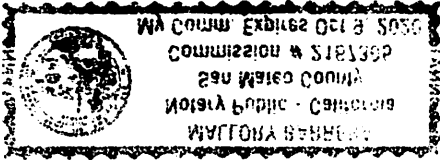
Title or Type of Document: Key Ceremony Script Document Date: 2.5.18  
Number of Pages: \_\_\_\_\_ Signer(s) Other Than Named Above: Bill Woodcock

**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: \_\_\_\_\_







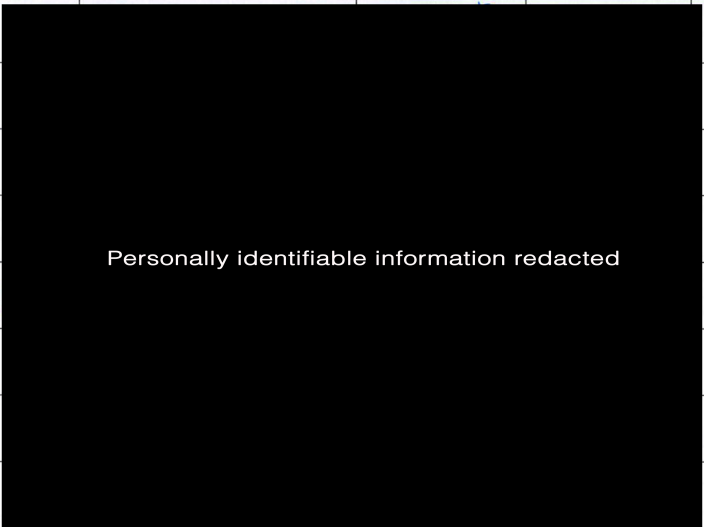
## 1600 Shattuck Avenue Facilities Sign-In Sheet

Role	Name	Signature	Date	Entry Time PST	Exit Time PST
FO4	Mohamed EL-BASHIR				
CA	Robert MARTIN- LEGENE				
SC1	Bill WOODCOCK				
EW3	Mallory BARRERA				
CO1	Steve FELDMAN				
CO4	Eric ALLMAN				
CO7	Gaurab UPADHAYA				
R	David HUDDLESTON				
R	James MITCHELL				

Personally identifiable information redacted

### Participant Signature Sheet

(Please have it signed at Exit Time)

Role	Name	Citizenship	Signature	Form of Identification	Identification Number	Date	Entry Time UTC	Exit Time UTC
CA	Robert Martin-Legene		 <p>Personally identifiable information redacted</p>			2/2/18	17:14	20:30
EW3	Mallory BARRERA					2/2/18	17:09	20:31
CO1	Steve Feldman					2/2/18	17:12	20:29
CO4	Eric ALLMAN					2/2/18	17:15	20:30
CO7	Gaurab UPADHAYA					2/2/18	17:10	20:29
SC1	Bill Woddcock					2/2/18	17:13	20:30
R	David HUDDLESTON					2/2/18	17:11	20:30
R	James MITCHELL					2/2/18	17:17	20:29

## **Appendix C: Abbreviations Used in This Document**

### **Roles**

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

### **Other Abbreviation**

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

## Appendix D: Letter and Number Pronunciation

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

## Appendix: E

### Card Distribution from Key Ceremony 1

DNSSEC Key Ceremony Script		Tuesday, April 26, 2011	
<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>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, Stephan 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	SMK 4, 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 26, 2011						
Smart Card Sign Out Sheet								
CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW	
-1	CO1	OP 1 of 7	A21095013	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	1/6
	CO1	SO 1 of 7	A21095012	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	1/6
	CO1	SMK 1 of 7	A21095011	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	1/6
	CO2	OP 2 of 7	A21095010	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	1/6
1	CO2	SO 2 of 7	A21095009	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	1/6
-1	CO2	SMK 2 of 7	A21095008	Michael SINATRA	<i>[Signature]</i>	4/25/11	20:55	1/6
	CO3	OP 3 of 7	A21095007	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	1/6
1	CO3	SO 3 of 7	A21095006	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	1/6
-1	CO3	SMK 3 of 7	A21095004	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:52	1/6
	CO4	OP 4 of 7	A21095005	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	1/6
1	CO4	SO 4 of 7	A21095003	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	1/6
-1	CO4	SMK 4 of 7	A21095002	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	1/6
	CO5	OP 5 of 7	A21095001	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:50	1/6
1	CO5	SO 5 of 7	A21095000	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	1/6
-1	CO5	SMK 5 of 7	A21094999	Steve FELDMAN	<i>[Signature]</i>	4/25/11	20:56	1/6
	CO6	OP 6 of 7	A21094998	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	1/6
1	CO6	SO 6 of 7	A21094997	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	1/6
-1	CO6	SMK 6 of 7	A21094996	Kim DAVIES	<i>[Signature]</i>	4/25/11	8:53	1/6
	CO7	OP 7 of 7	A21094995	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	1/6
1	CO7	SO 7 of 7	A21094994	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	1/6
-1	CO7	SMK 7 of 7	A21094993	Jonny MARTIN	<i>[Signature]</i>	4/25/11	8:58	1/6



**Appendix: G**

**Smart Card Sign Out Sheet from Key Ceremony 2**

DNSSEC Key Ceremony Script Monday, May 30, 2011

**Smart Card Sign Out Sheet**

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EB#
A19204943	CO1 OP 1 of 7	A19204935	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<i>[EB#]</i>
	CO1 SO 1 of 7	A19204934	Steve FELDMAN	<i>[Signature]</i>	5/30/11	0047	<i>[EB#]</i>
	CO1 SMK 1 of 7		Steve FELDMAN		5/30/11		
A19204942	CO2 OP 2 of 7	A19204933	Michael SINATRA	<i>[Signature]</i>	5/30/11	0049	<i>[EB#]</i>
	CO2 SO 2 of 7	A19204931	Michael SINATRA	<i>[Signature]</i>	5/30/11	0049	<i>[EB#]</i>
	CO2 SMK 2 of 7		Michael SINATRA		5/30/11		
A19204941	CO4 OP 4 of 7	A19204932	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<i>[EB#]</i>
	CO4 SO 4 of 7	A19204930	Jonny MARTIN	<i>[Signature]</i>	5/30/11	0050	<i>[EB#]</i>
	CO4 SMK 4 of 7		Jonny MARTIN		5/30/11		
A19204940	CO5 OP 5 of 7	A19204929	Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<i>[EB#]</i>
	CO5 SO 5 of 7	A19204928	Steve SOMOGYI	<i>[Signature]</i>	5/30/11	0051	<i>[EB#]</i>
	CO5 SMK 5 of 7		Steve SOMOGYI		5/30/11		
	CO7 OP 7 of 7		Jonny MARTIN		5/30/11		
	CO7 SO 7 of 7		Jonny MARTIN		5/30/11		
	CO7 SMK 7 of 7		Jonny MARTIN		5/30/11		

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

Packet Clearing House Page 25 of 32




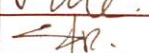
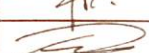
## Appendix: H

### Smart Card Sign Out Sheet from Key Ceremony 3

DNSSEC Key Ceremony Script

Monday, June 20, 2011

#### Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	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.	Tf	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	Tf
CO2	SO 2 of 7	A19204952	Michael SINATRA	<i>Michael S. Sin</i>	1/20/12	2051	Tf
CO4	OP 4 of 7	A19204949	Jonny MARTIN	<i>Jonny</i>	1/20/12	2049	Tf
CO4	SO 4 of 7	A19204953	Jonny MARTIN	<i>Jonny</i>	1/20/12	2049	Tf
CO5	OP 5 of 7	A19204951	Stephan SOMOGYI	<i>Stephan</i>	1/20/12	2016	Tf
CO5	<del>OP</del> SO 5 of 7 Bag	A19204954	Stephan SOMOGYI	<i>Stephan</i>	1/20/12	2016	Tf

OUTSIDE BAG













## Appendix: J

### Smart Card Sign Out Sheet from Key Ceremony 5


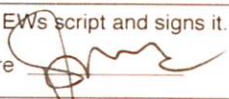

DNSSEC Key Ceremony Script

Friday, April 27, 2012


#### Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A19204955	Steve FELDMAN		4/27/12	18:44	
CO1	<sup>Outer</sup> SO 1 of 7 bag	3112567	Steve FELDMAN		4/27/12	18:44	
CO3	OP 3 of 7	A3112566	Kim DAVIES		4/27/12	18:46	
CO3	<sup>Outer</sup> 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	<sup>Outer</sup> 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

## Appendix: K

### Smart Card Sign Out Sheet from Key Ceremony 5-1

DNSSEC Key Ceremony Script

Wednesday, May 30, 2012

#### Re-Distribution of Cards

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

#### Smart Card Sign Out Sheet

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

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

DNSSEC Key Ceremony Script

Friday, July 27, 2012

### Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
67	CA calls each CO to return their smartcards. As each CO receives and inspects their cards, they fill out the sign out sheet below and EW initials their entry. Note new outer bags in sheet below.	TH	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	TH
CO1	<del>Outer 1 of 7</del>		Steve FELDMAN		<del>7/27/12</del>		
CO4	OP 4 of 7	A28410814	Jonny MARTIN	<i>[Signature]</i>	7/27/12	2019	TH
CO4	<del>Outer 4 of 7</del>		Jonny MARTIN		<del>7/27/12</del>		
CO5	OP 5 of 7	A28410817	Stephan SOMOGYI	<i>[Signature]</i>	7/27/12	2019	TH
CO5	<del>Outer 5 of 7</del>		Stephan SOMOGYI		<del>7/27/12</del>		

## 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.	TH	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.	TH	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	2045	TH
CO2	OP 2 of 7	A28410804	Michael SINATRA	<i>[Signature]</i>	12/14/12	2046	TH
CO4	OP 4 of 7	A28410803	Jonny MARTIN	<i>[Signature]</i>	12/14/12	2046	TH

## Appendix: N

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

DNSSEC Key Ceremony Script		Thursday, September 12, 2013					
<b>Re-Distribution of Cards</b>							
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				
<b>Smart Card Sign Out Sheet</b>							
CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410802	Steve FELDMAN		9/12/13	1822	1/1
CO2	OP 2 of 7	A28410801	Michael SINATRA		9/12/13	1816	1/1
CO3	OP 3 of 7	A28410800	Kim DAVIES		9/12/13	1819	1/1
<b>Sign-Out on Participant Signature Sheet</b>							
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				
<b>Sign Out of Facility</b>							
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	3:58 PM				
<b>Stop Audio-Visual Recording</b>							
Step	Activity	Initial	Time (PDT)				
67	SA stops audio and video recording.	1/1	4:00 PM				
Packet Clearing House		Page 12 of 29					



## Appendix: O

### Smart Card Sign Out Sheet from Key Ceremony 9

DNSSEC Key Ceremony Script

Friday, January 10, 2014




#### Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
35	CA places each OP card with pre-printed warning slip in its own new TEB and records the TEB # in the EW's copy of the smart card sign out sheet below, reading it aloud for verification and giving the TEB tear-off strip to the EW.	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		1/10/14	18:16	ff
CO2	OP 2 of 7	A28410773	Michael SINATRA		1/10/14	18:17	ff
CO5	OP 5 of 7	A28410772	Stephan SOMOGYI		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

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.	<i>MS</i>	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.	<i>MS</i>	0845

#### Smart Card Sign Out Sheet

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

#### Optionally leave facility

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

## 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

### Smart Card Sign Out Sheet from Key Ceremony 12

DNSSEC Key Ceremony Script

Monday, February 9, 2015

#### Re-Package OP Cards

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

#### Re-Distribution of Cards

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

#### Smart Card Sign Out Sheet


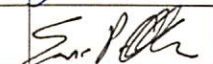

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
C03	OP 3 of 7	A28410758	Kim DAVIES	<i>[Handwritten Signature]</i>	2/9/15	0747	<i>[Handwritten Initials]</i>
C06	OP 6 of 7	A28410767	LEE Han-Chuan	<i>[Handwritten Signature]</i>	2/9/15	0747	<i>[Handwritten Initials]</i>
C07	OP 7 of 7	A28460766	Gaurab UPADHAYA	<i>[Handwritten Signature]</i>	2/9/15	0748	<i>[Handwritten Initials]</i>

#### Optionally leave facility

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

## Appendix: S

### Smart Card Sign Out Sheet from Key Ceremony 13

DNSSEC Key Ceremony Script		Friday, September 25, 2015					
<b>Re-Package OP Cards</b>							
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.	H	19:14				
<b>Re-Distribution of Cards</b>							
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.	H	19:20				
<b>Smart Card Sign Out Sheet</b>							
CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A28410724	Steve FELDMAN		9/25/15	19:15	H
CO4	OP 4 of 7	A28410725	Eric ALLMAN		9/25/15	19:16	H
CO5	OP 5 of 7	A28410726	Stephan SOMOGYI		9/25/15	19:16	H
<b>Optionally leave facility</b>							
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.	H	19:34				
Packet Clearing House		Page 10 of 38					


## Appendix: T

### Smart Card Sign Out Sheet from Key Ceremony 14


DNSSEC Key Ceremony Script

Monday, November 23, 2015



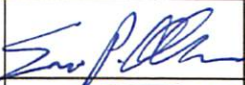



#### Re-Package OP Cards

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


#### Re-Distribution of Cards

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

#### Smart Card Sign Out Sheet

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

#### Optionally leave facility

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

# Appendix: U

## Smart Card Sign Out Sheet from Key Ceremony 15

DNSSEC Key Ceremony Script

Friday, July 8, 2016

### PCH DNSSEC Key Ceremony Script Exception Form

The Smart Card Sign Out Sheet automatically generated on page 27 of 62 of this script included only rows for OP cards, but needs rows for SO and SMK cards as well. APP cards are separately bagged in a different step, and AAK cards will be destroyed before the end of the ceremony.

### Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	A 28410760	Steve FELDMAN		7/8/16	00:27 UTC	
CO1	SO 1 of 7	A 28410759	Steve FELDMAN		7/8/16	00:27 UTC	
CO1	SMK 1 of 7	A28410761	Steve FELDMAN		7/8/16	00:27 UTC	
CO2	OP 2 of 7	A28410753	Michael SINATRA		7/8/16	00:29 UTC	
CO2	SO 2 of 7	A28410752	Michael SINATRA		7/8/16	00:29 UTC	
CO2	SMK 2 of 7	A28410751	Michael SINATRA		7/8/16	00:29 UTC	
CO3	OP 3 of 7	A28410749	Kim DAVIES		7/8/16	20:39 UTC	
CO3	SO 3 of 7	A28410748	Kim DAVIES		7/8/16	20:39 UTC	
CO3	SMK 3 of 7	A28410747	Kim DAVIES		7/8/16	20:39 UTC	
CO4	OP 4 of 7	A28410750	Eric ALLMAN		7/8/16	00:33 UTC	
CO4	SO 4 of 7	A28410737	Eric ALLMAN		7/8/16	00:33 UTC	
CO4	SMK 4 of 7	A28410742	Eric ALLMAN		7/8/16	00:33 UTC	
CO7	OP 7 of 7	A 28410746	Gaurab UPADHAYA		7/8/16	20:40 UTC	
CO7	SO 7 of 7	A28410745	Gaurab UPADHAYA		7/8/16	20:40 UTC	
CO7	SMK 7 of 7	A28410744	Gaurab UPADHAYA		7/8/16	20:40 UTC	

## Appendix: V

### Smart Card Sign Out Sheet from Key Ceremony 16

DNSSEC Key Ceremony Script

Wednesday, August 17, 2016

#### Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
32	CA places each OP card with pre-printed warning slip in its own new TEB and reads the TEB number aloud. The EW records each TEB number in the smart card sign out sheet in the EW copy of the script, reading it aloud for verification.	<i>EW</i>	17:34

#### Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
33	CA calls each CO to retrieve their smart cards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet and the EW initials each entry.	<i>EW</i>	17:36

#### Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	BB7170519 <sup>P</sup>	Steve FELDMAN	<i>[Signature]</i>	8/17/16	17:35	<i>EW</i>
CO4	OP 4 of 7	BB71705191	Eric ALLMAN	<i>[Signature]</i>	8/17/16	17:36	<i>EW</i>
CO5	OP 5 of 7	BB71705192	Stephan SOMOGYI	<i>[Signature]</i>	8/17/16	17:36	<i>EW</i>

#### Optionally leave facility

Step	Activity	Initial	Time (UTC)
34	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.	<i>EW</i>	17:45




## Appendix: W

### Smart Card Sign Out Sheet from Key Ceremony 17


DNSSEC Key Ceremony Script

Wednesday, December 14, 2016

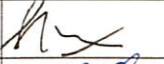





#### Re-Package OP Cards

Step	Activity	Initial	Time (UTC)
32	CA places each OP card with pre-printed warning slip in its own new TEB and reads the TEB number aloud. The EW records each TEB number in the smart card sign out sheet in the EW copy of the script, reading it aloud for verification.		18:38


#### Re-Distribution of Cards

Step	Activity	Initial	Time (UTC)
33	CA calls each CO to retrieve their smart cards. As each CO receives and inspects their cards, they verify, date and sign the EW's copy of the sign out sheet and the EW initials each entry.		18:42

#### Smart Card Sign Out Sheet

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	EW
CO1	OP 1 of 7	BB71705260	Steve FELDMAN		12/14/16	18:42	
CO4	OP 4 of 7	BB71705261	Eric ALLMAN		12/14/16	18:41	
CO7	OP 7 of 7	BB71705262	Gaurab UPADHAYA		12/14/16	18:41	

#### Optionally leave facility

Step	Activity	Initial	Time (UTC)
34	Optionally, all participants can now leave the room if the room is closed and sealed until everyone's return.		18:44

# Appendix: X





## Smart Card Sign Out Sheet from Key Ceremony 18

DNSSEC Key Ceremony Script

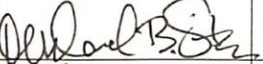
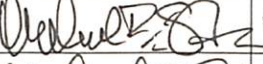
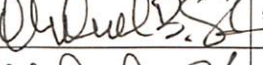

Thursday, September 28, 2017

Key Ceremony 18  
Smart Card Sign Out Sheet

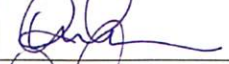



CO1 Steve FELDMAN

TEB #	Containing	Signature	Date	Time	EW
RA02070101	OP1 of 7		9/28/17	18:09	MAB
RA02070107	SO1 of 7		9/28/17	18:10	MAB
RA02070109	SMK1 of 7		9/28/17	18:11	MAB
AE20992104	Card Case 1		9/28/17	18:13	MAB

CO2 Michael SINATRA

TEB #	Containing	Signature	Date	Time	EW
RA02070179	OP2 of 7		9/28/17	18:15	MAB
RA02070187	SO2 of 7		9/28/17	18:15	MAB
RA02070171	SMK2 of 7		9/28/17	18:10	MAB
AE20992100	Card Case 2		9/28/17	18:17	MAB

CO3 Kim DAVIES

TEB #	Containing	Signature	Date	Time	EW
RA02070199	OP3 of 7		9/28/17	18:19	MAB
RA02070105	SO3 of 7		9/28/17	18:20	MAB
RA02070173	SMK3 of 7		9/28/17	18:20	MAB
AE20992108	Card Case 3		9/28/17	18:21	MAB

## Appendix: Y

### Boot-DVD Checksum from Key Ceremony 6

DNSSEC Key Ceremony Script		Friday, July 27, 2012	
16	CA opens a terminal window.	✓	17:18
17	<p>CA verifies the time zone, date, and time on the laptop and synchronizes it if necessary.</p> <p>Display the current time and timezone:</p> <pre>date</pre> <p>If the timezone is not set to UTC:</p> <pre>cd /etc/ rm localtime ln -s /usr/share/zoneinfo/UTC localtime</pre> <p>Set time to match the wall clock:</p> <pre>date mmddHHMMYYYY</pre> <p>Verify:</p> <pre>date</pre>	✓	17:20
18	<p>CA calculates sha256 checksum of the boot-DVD. CA may proceed with additional steps while this process completes. When the checksum is complete, CA reads it aloud, four digits at a time.</p> <pre>sha256sum /dev/cdrom</pre>	✓	17:34
19	<p>EW records the sixty-four digit boot-DVD checksum</p> <pre>7DE4 31F9 C33D 0FFF 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 1, reproduced for convenience in the appendices of this document.</p>	✓	17:34
20	CA connects USB hub to laptop.	✓	17:21
21	CA removes HSMFD KSK-HSM-01B-SJC from TEB and plugs into a free USB slot on the laptop; waits for O/S to recognize the FD. CA lets participants view contents of HSMFD then closes FD window.	✓	17:29

*ROTATED SCHEDULES FOR FIRST RUNS*